

UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
BACHARELADO EM CIÊNCIAS DA COMPUTAÇÃO

REPUTAÇÃO DIGITAL:
CONFIABILIDADE E IDENTIDADE EM UM MUNDO
TRANSPARENTE

Eduardo Felipe Castegnaro

Florianópolis - SC

2009 / 2

Eduardo Felipe Castegnaro

REPUTAÇÃO DIGITAL:
CONFIABILIDADE E IDENTIDADE EM UM MUNDO TRANSPARENTE

Trabalho de Conclusão de Curso submetido à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Bacharel em Ciências da Computação

Florianópolis - SC

2009 / 2

REPUTAÇÃO DIGITAL:
CONFIABILIDADE E IDENTIDADE EM UM MUNDO TRANSPARENTE

Eduardo Felipe Castegnaro

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Ciências da Computação e aprovado em sua forma final pelo Departamento de Informática e Estatística da Universidade Federal de Santa Catarina.

Data de aprovação: 04 de dezembro de 2009.

Prof. Dr. Luís Fernando Friedrich.
Universidade Federal de Santa Catarina
Coordenador do Curso

Banca Examinadora:

Prof. José Eduardo De Lucca
Universidade Federal de Santa Catarina

Prof. Dr. Bernardo Gonçalves Riso
Universidade Federal de Santa Catarina

Prof. Dr. Vitorio Bruno Mazzola
Universidade Federal de Santa Catarina

Dedico esse trabalho à minha mãe, Rosângela.

Quando eu crescer quero ser igual a você.

Agradecimentos

Ao professor José Eduardo De Lucca, por ter me orientado e tolerado os meus infinitos atrasos.

Ao professor Bernardo Riso, por ter oferecido valiosas correções e sugestões.

A D. Hardt, J. Bufu, J. Hoyt, criadores e mantenedores do protocolo *openid-attribute-exchange*, cuja estrutura e organização geral foi utilizada como modelo de referência para a criação do novo protocolo.

A Jeff Atwood, que gentilmente cedeu os dados sobre os usuários de seu site Stackoverflow para que pudesse servir como exemplo da modelagem sugerida de reputação digital.

E especialmente aos meus amigos Cecilia Giuffra e Alex de Magalhães, por terem ouvido as dores do parto desse trabalho.

Sumário

Lista de figuras	9
Resumo	10
Abstract	11
1 Introdução	12
1.1 Escopo desse trabalho	13
2 Identidade de uma entidade	14
2.1 Identidade social	14
2.2 Identidade Digital	16
2.3 OpenID	20
2.4 Histórico do OpenID	21
2.5 OpenID 2.0	23
2.5.1 Visão geral da arquitetura do protocolo	24
2.5.2 A primeira camada: Identificadores	24
2.5.3 A segunda camada: Descobrimto de serviços	25
2.5.4 A terceira camada: Autenticação	26
2.5.5 A quarta camada: Transporte de dados	27
2.6 Exemplo de Fluxo do Protocolo OpenID	28
2.7 Problemas com o protocolo	31
3 Yadis	31
3.1 Uma visão geral do protocolo	33
3.2 Formato do documento Yadis	34
4 Reputação Digital	37
4.1 O que é reputação	38
4.2 A Fragilidade da reputação	42
4.2.1 Do dinamismo da reputação	42

4.3 Considerações adicionais sobre reputação online	46
4.3.1 Pseudônimos	46
4.3.2 Manipulação estratégica de mecanismos de reputação.....	47
4.4 Alternativas arquiteturais para reputação	49
4.4.1 Formação de reputação implicitamente.....	49
4.4.2 Arquiteturas descentralizados de reputação	50
5 Estudo de caso: Comunidade Stack Overflow	51
5.1 Distribuição da reputação na comunidade	52
5.2 Insígnias de reputação	55
6 Proposta de extensão: OpenID Reputation Exchange	58
6.1 Terminologia.....	58
6.1.1 Definições e Convenções	58
6.2 Visão geral.....	59
6.3 Modelo de Informação	61
6.3.1. Identificador Pessoal.....	62
6.3.2. Valor de Reputação.....	62
6.3.3. Identificador de Tipo do Emblema de Reputação	62
6.4 Descoberta	63
6.5 Mensagem Fetch.....	63
6.5.1 Formato da mensagem.....	63
6.5.2 Formato da resposta.....	65
6.5.2.1 Sucesso	65
6.5.2.2 Falha.....	68
6.6 Mensagem List	68
6.6.1 Lista Pedido Formato	69
6.6.2 Lista Response Format.....	69
6.6.2.1 Sucesso	69
6.6.2.2 Falha.....	70

6.7 Mensagem Add	71
6.7.1 Formato da mensagem Add.....	71
6.7.2 Formato de resposta.....	71
6.7.2.1 Sucesso.....	71
6.7.2.2 Falha.....	72
6.8 Considerações de Segurança.....	72
Conclusões e trabalhos futuros	73
Referências bibliográficas	74

Lista de figuras

Figura 1 - Stack do Protocolo OpenID	24
Figura 2: Fluxo básico da autenticação no protocolo OpenID	27
Figura 3 - Fornecimento do identificador	29
Figura 4 - Aceitando fornecer identificador	30
Figura 5 - Verificando login	30
Figura 6 - Permitindo o fornecimento de atributos	31
Figura 7 - Distribuição da reputação no site Stack Overflow	52
Figura 8 - Distribuição da reputação por ação autorizada	54
Figura 9 - Distribuição de insígnias no site Stack Overflow	57
Figura 10 - Visão geral da interação com o protocolo OpenID 2.0	61

Resumo

Com a disseminação de serviços web houve, também, uma explosão no número de nomes de usuários e senhas que um indivíduo precisa manter para permitir a autenticação em todos esses serviços. Criou-se, então, um protocolo denominado OpenID que permite o reuso de uma identidade em múltiplos serviços de maneira segura. O protocolo já foi adotado por grandes empresas, como *Microsoft* e *Google*.

Desde sua segunda versão o protocolo permite extensões através da troca de novas mensagens pelas múltiplas partes nele envolvidas. Um exemplo é a extensão *Attribute Exchange*, que permite a troca de informações sobre o usuário, como e-mail e data de nascimento. A reputação de um usuário, ou seja, o quão valioso ele é para uma comunidade, não é passível de transmissão via *Attribute Exchange*.

Este trabalho apresenta a especificação de uma nova extensão ao protocolo OpenID que propicia um modelo de reputação distribuída com o intuito de unificar a reputação de um usuário da mesma forma que a sua identidade foi unificada com o protocolo original. Desse modo evita-se a criação de ilhas de reputação e permite-se o uso da extensão como fator decisivo no processo de utilização da reputação como atributo autorizador.

Durante o desenvolvimento do trabalho foram estudados diferentes modelos de reputação distribuída, tendo por fim sido criado um modelo baseado na implementação presente no site StackOverflow.

Palavras-Chave: Reputação digital, Sistemas de Reputação, Protocolos de identidade, OpenID.

Abstract

With the wide spread adoption of web services there was an explosion of usernames and passwords a subject must keep in order to authenticate with all those services. A protocol named OpenID was then created to allow the safe reuse of a single identity in multiple services. The protocol has been implemented by big companies like *Microsoft* and *Google*.

Since it's second version the protocol allow extensions though the exchange of new messages by the involved parties. One example is *Attribute Exchange*, an extension that allows the exchange of user information, such as e-mail and date of birth. A user's reputation, which represents how valuable one is to a community, can't be exchanged via *Attribute Exchange*.

This paper presents the specification of a new extension that leads to a distributed reputation model based on OpenID, with the intent of unifying a user's reputation the same way a it's identity was unified with the original protocol, therefore halting the creation of islands of reputation and allow it's use as a factor in authorization.

During the writing of this paper several reputation models were studied and the one proposed is similar to the implementation present on [StackOverflow.com](https://stackoverflow.com).

Keywords: Digital Reputation, Reputation System, Identity Protocol, OpenID

1 Introdução

Analisando-se tendências e padrões disseminados em sociedades ao redor do mundo, desde que a internet tornou-se epidêmica, é possível determinar uma mudança topológica na estrutura dos grupos básicos que apresentam tais tendências e padrões.

As sociedades costumavam ser estruturadas com base em contatos diretos, principalmente verbais, entre seus membros, em que alguns indivíduos controlavam os recursos escassos e a informação e os disponibilizavam, exercitando sobre eles seu poder de distorção.

O que o uso disseminado da Internet tornou possível foi a mudança de uma estrutura hierárquica local e presencial, para uma estrutura auto-organizável, plana, formada principalmente por grupos desconexos, mas em escala global, onde a posição geográfica do indivíduo é irrelevante para sua atuação na comunidade. Como esses grupos não compartilham identidade, reputação ou qualquer outra informação baseada na individualidade de seus membros, um mesmo indivíduo pode ter múltiplas identidades, desconexas, e múltiplas reputações. Nada impede que um indivíduo prestativo em uma determinada comunidade possa ser simultaneamente vândalo em outra comunidade.

Soluções para esse problema relativo a múltiplas identidades e sua confiabilidade entre grupos e indivíduos foram propostas, entre elas o OpenID, que elimina a necessidade da existência de múltiplas identidades, simplificando a experiência online, fornecendo transparência e identificabilidade.

Durante a transição para identidades em um mundo digital, a idéia de privacidade baseada em confidencialidade, fornecendo confiança e segurança, foi modificada para um mundo de privacidade baseada em transparência, também capaz de fornecer confiança e segurança, através do controle da informação disponível baseado em quem solicita a informação. Privacidade em um mundo digital não é anonimidade, e sim um gerenciamento sutil da identidade, permitindo manter privados os dados não essenciais, relativos ao indivíduo naquele contexto.

O protocolo OpenID, usado para autenticação, não possui noção de reputação, e apenas recentemente incluiu a possibilidade de associar atributos a uma identidade. Porém os atributos são armazenados no provedor de identidade,

diminuindo a confiança do Consumidor de Identidade naquela informação, uma vez que o usuário tem controle direto dela.

Houve tentativas anteriores para estabelecimento de confiabilidade distribuída, como por exemplo o sistema PGP, que foram bem populares no final da década de 90, mas tem seu uso restrito a usuários avançados.

Pode-se observar que um indivíduo valioso dentro de uma comunidade é possivelmente valioso dentro de várias outras comunidades. Sendo assim é interessante que uma reputação possa ser compartilhada, e indivíduos possam ter direitos automáticos entre comunidades, favorecendo a contribuição a múltiplos projetos, fato raramente observado hoje em dia. Para tanto é necessário que exista confiabilidade entre comunidades, e entre indivíduos que delas participam.

Uma das grandes limitações do protocolo atual é que as comunidades são passivas em relação a identidade dos seus membros. Não podem associar informações à identidade, compartilhando-as com outras comunidades. A identidade é caminho de mão única, em que o indivíduo informa quem é, mas não permite que a comunidade diga o mesmo.

1.1 Escopo desse trabalho

Explorar e entender a capacidade tecnológica atual que possibilita a criação de uma identidade digital móvel, capaz de fornecer não só single sign-on, mas também outras funcionalidades, estendendo-a para permitir a criação de uma reputação digital e sua manutenção entre comunidades desconexas, mantendo a privacidade, transparência e flexibilidade de uma existência como ser sócio-digital.

A fim de estudar a interação comunidade/indivíduo com reputação, especifica-se um modelo de reputação distribuída baseada no protocolo OpenID. O modelo será baseado em um estudo de caso de uma comunidade bem sucedida que utiliza a reputação como fator decisivo para a escalada de privilégios, ou seja, quanto maior a reputação mais ações o usuário tem permissão para executar dentro da comunidade.

Sendo assim, o propósito desse trabalho é propor uma extensão ao protocolo OpenID, permitindo a criação de uma reputação global, associada a uma identidade, que possa ser compartilhada por todas as comunidades e serviços de que o proprietário da identidade participa. Estudos serão propostos sobre como tal

mecanismo pode ser modelado, como uma comunidade deve poder influenciar na reputação de um indivíduo, e como o indivíduo ainda mantém o controle de sua identidade nesse cenário.

O protocolo proposto será especificado via RFC que permite definir o modelo de interação das múltiplas entidades envolvidas no processo de agregação da reputação de um indivíduo.

A motivação por trás dessa extensão vem principalmente do modelo de contribuição para projetos de software livre. O modelo adotado atualmente prevê que um indivíduo deve se mostrar digno de confiança e suficientemente capacitado para contribuir para um projeto e, conseqüentemente, estaria apto a contribuir em outros projetos que compartilham da mesma comunidade, ou que possuem comunidades próximas.

2 Identidade de uma entidade

2.1 Identidade social

A palavra identidade traz no seu conceito a noção de perfeitamente igual ou semelhante. No entanto, esta definição serve muito mais como um complicador quando usada para definir o conceito de identidade individual dentro de uma sociedade. Não é possível juntar categorias ou tipos ideais para então defini-los. É no diálogo travado constantemente entre a essência do indivíduo, seu eu interior, sua interação com a sociedade, com os grupos culturais que o cercam que se formará a sua identidade perante a sociedade.

Na concepção sociológica de identidade está presente a subjetividade.

Desse ponto de vista, a identidade nada mais é que o resultado a um só tempo estável e provisório, individual e coletivo, subjetivo e objetivo, biográfico e estrutural, dos diversos processos e socialização que, conjuntamente, constroem os indivíduos e definem instituições. (Dubar, 2005, p. 136)

É na infância, no processo de socialização com a família e principalmente na relação com a mãe, que a criança aprende a ser humano e forma a sua identidade. E ao iniciar sua vida escolar na relação com os outros que farão parte de sua vida que ela constrói a sua primeira identidade social. Os processos acima citados são chamados de aparelhos de socialização primária (família e escola). Os chamados aparelhos de socialização secundária acontecem ao longo da vida adulta, nas

empresas, profissões. Portanto, pode-se concluir que a identidade é um produto da socialização. “É exatamente na compreensão interna das representações cognitivas e afetivas, perceptivas e operacionais, estratégicas e identitárias que reside a chave da construção operacional das identidades” (Dubar, 2005, p. 129).

É a partir desta interação com os outros que o indivíduo passa a ser identificado, de tal modo que ele pode incorporar ou refutar essa identificação que recebe dos outros e das instituições. São dois processos identitários heterogêneos. O primeiro, trata de identidades sociais conferidas pelas instituições na relação com os indivíduos. O segundo processo trata daquilo que o indivíduo diz como sendo a sua história, tornando-o assim construtor de sua própria identidade.

É, portanto, nesta relação que pode ser chamada de dialética, entre o indivíduo e a sociedade, que se constrói a identidade social. No entanto, a construção das identidades nesta relação é complexa e delicada. Dubar (2005) chama de processo biográfico ou identidade para si aquela herdada pelo indivíduo. E de processo relacional ou identidade para o outro aquela construída nas relações com outros ou instituições. Este processo leva à formação básica de reputação de um indivíduo. Esta relação é problemática na medida em que se constrói na aceitação ou na refutação da identidade que foi proposta, atribuída ao indivíduo e na identidade subjetiva, aquela visada pelo indivíduo. Dentro dessa negociação identitária a qualidade das relações com o outro aparece como elemento chave no movimento das identidades.

O problema da construção da identidade reside no fato de enxergar estes dois processos de forma estanque e harmonioso, onde o indivíduo terá uma trajetória pré-estabelecida dentro da sociedade. Quando, na verdade, nenhum processo organizacional, institucional, ou macrossocial garante que esta trajetória proporcionará a existência de identidades iguais hoje e no futuro.

Trata-se de reconhecer que o problema da identidade sinaliza a importância de perceber as mediações entre agente social e sociedade, entre os processos macro e microssociais. O que se propõe como foco analítico não é nem o indivíduo nem as estruturas sociais em si mesmas, senão a relação entre indivíduo e sociedade (Mitjavila, 1994).

Ainda assim, os dois processos de formação de identidade utilizam um mecanismo comum, a tipificação, ou seja, há um determinado número de modelos

significativos socialmente com os quais se podem realizar combinações coerentes. Esses modelos variam de acordo com os espaços, a temporalidade biográfica e histórica em que se desenvolvem. Podem combinar ainda critérios de pertencimento, como trabalho – posição profissional – com o tipo e nível de estudos escolares realizados, conferindo legitimidade a essas categorias, efetivamente fundindo as noções de reputação e identidade.

Os modelos ou categorias pré-definidos tendem sempre à desatualização. A proximidade entre a identidade virtual e real é tão mais pertinente quanto mais se utilizam e aceitam as categorias oficiais de identificação. A negociação permanente e complexa com as instituições pertinentes e categorias oficiais é que produzirá, de fato, a identidade que prevalecerá.

A construção de uma identidade social e reputação, chamada de processo biográfico, é construída na família, escola, mercado de trabalho e na empresa. É a transação subjetiva. Já o processo identitário relacional acontece quando o indivíduo tem o reconhecimento de suas competências, do potencial do seu conhecimento, com a possibilidade de investir, de negociar e administrar em espaços considerados legítimos para a identificação dos sujeitos. Chama-se transação objetiva. Portanto o processo identitário biográfico e o processo identitário relacional, articulados, orientam a trajetória de uma geração. Mas cada geração constrói sua própria identidade social, podendo ter bases nas que as precederam, assim como construindo novas estratégias ao longo de suas vidas (Dubar, 2005).

2.2 Identidade Digital

A identidade de um indivíduo em um mundo digital é representada por um conjunto de atributos (Bhargav-Spantzel, Camenisch *et al.*, 2006). Esses atributos podem simplesmente ser afirmações feitas por um usuário que ainda não foram verificadas por uma terceira parte ou podem ser atributos já verificados e confirmados por uma terceira parte confiável. Um indivíduo pode potencialmente ter várias identidades diferentes, correspondendo a diferentes conjuntos de atributos relacionados (Bhargav-Spantzel, Camenisch *et al.*, 2006).

Um atributo pode ser visto como uma característica associada com uma entidade, como por exemplo um indivíduo (Camp, 2004). Exemplos de atributos persistentes são cor dos olhos e data de nascimento. Exemplos de atributos

temporários incluem endereço, empregador e salário. O Cadastro de Pessoa Física é considerado exemplo de um atributo de longa duração dentro do sistema de governo do Brasil. Números de Passaporte são considerados internacionalmente como atributos de longa duração.

Identidade digital, segundo Cameron, é “um conjunto de afirmações feitas por um indivíduo digital sobre ele mesmo ou sobre outro indivíduo digital, sendo que um indivíduo digital é uma pessoa ou entidade representada ou existente no universo digital que está sendo descrita ou com a qual se está lidando” (Cameron, 2005). Em contrapartida Camp vê identidade digital, em um sistema de gerenciamento de identidade, como o conjunto de atributos de longa duração associados a uma entidade (Camp, 2004).

Para Cameron grande parte do processo decisório existente em computação distribuída é derivada do resultado de “lidar com” uma requisição proveniente de outra entidade (Cameron, 2005). É necessário reafirmar que o mundo digital inclui vários outros seres com que precisamos interagir que não são necessariamente seres humanos, incluindo:

- * Dispositivos e computadores (que nos permitem interagir com o mundo digital);
- * Recursos digitais (que nos atraem para o mundo digital); e
- * Políticas e relacionamentos já existentes entre outros seres digitais (primariamente entre humanos, mas possivelmente entre dispositivos).

Cameron também considera que uma afirmação nesse contexto pode ser vista como “Uma asserção sobre a veracidade de algo, tipicamente algo que está sendo disputado ou posto em dúvida” (Cameron, 2005).

É comum identidades carregarem consigo identificadores, que as distinguem, em um contexto, de qualquer outra pessoa, lugar ou entidade dentro do mesmo contexto (Camp, 2004). Por exemplo: um carro tem uma placa de licenciamento como identificador, uma conta corrente tem um número e uma pessoa pode ser associada a uma série de informações, como CPF, carteira de identidade ou de motorista. Uma pessoa ou entidade pode ter uma multitude de identificadores. Um carro tem um número de série permanente, impresso no chassis do carro, e um número de placa temporário, ligado ao dono do carro. Cada identificador só é significativo no seu próprio contexto e só quando está diretamente associado a uma

entidade que está sendo identificada. Considerando isso, é possível considerar um identificador como sendo globalmente único caso seja composto da coisa a ser identificada mais contexto mais identificador.

Identificadores pessoais são identificadores persistentes que estão associados com um indivíduo em particular que são baseados em atributos difíceis ou impossíveis de se modificar (Camp, 2004). Um exemplo seria a data de nascimento e o valor de certos marcadores genéticos presentes no DNA. Perceba que, enquanto é possível mentir sobre a data de nascimento de uma pessoa, é impossível mudá-la. Identificadores pessoais não necessariamente são bons autenticadores.

Alguns tipos de afirmações acerca da identidade de uma entidade comuns no mundo digital:

- * Afirmação trazendo um identificador, por exemplo, que o número de matrícula da entidade que faz a afirmação é 0523219-8, ou que seu nome é “Eduardo Felipe Castegnaro”. É assim que muitos sistemas de identidade funcionam;

- * Uma outra afirmação pode dizer que a entidade sabe uma determinada senha secreta e é capaz de demonstrar o seu conhecimento dela;

- * Um conjunto de afirmações pode contemplar informações que podem, de maneira não ambígua, identificar uma entidade: Nome, data de nascimento, endereço e cidadania, por exemplo; e

- * A afirmação que a entidade pertence a um determinado grupo, como por exemplo dos homens com menos de 25 anos de idade.

Uma afirmação pode ainda indicar uma habilidade possuída pela entidade como, por exemplo, fazer um certo número máximo de requisições ou modificar um arquivo (Cameron, 2005).

Já, o conceito de “posto em dúvida” consegue expressar as sutileza de um mundo identitariamente disperso, como a Internet. Afirmações feitas em sistemas dispersos necessitam ser avaliadas pelos indivíduos que delas dependem. Quanto mais dispersa e aberta a participação uma rede se torna, mais evidente essa necessidade.

Nesse contexto, afirmações necessitam de uma constante descrença sobre elas. Não apenas descrença sobre se elas foram transmitidas do emissor para o

receptor intactas, mas também descrença sobre sua veracidade ou até mesmo relevância.

Esse processo de por em dúvida e verificar a identidade de uma entidade é chamado identificação. Por exemplo, “Você é o João da Silva” (Camp, 2004). Exemplos mais genéricos incluem admitir a associação entre uma pessoa e o nome que ela diz ter, determinar a associação entre uma empresa e um registro financeiro, conectar um paciente com o registro de um médico. A identificação ocorre dentro da rede baseada na individualidade de uma entidade, humana ou de computador. A identificação geralmente requer um identificador, como número do CPF ou passaporte.

Autenticar uma identidade é provar uma associação entre uma entidade e um identificador (Camp, 2004). Exemplo: a associação de uma pessoa com um registro estudantil, associação de um número de placa com um veículo ou uma pessoa com uma conta bancária. Em essência, essa é a verificação que a entidade é quem diz ser nesse contexto. É importante notar que enquanto “Você é João da Silva” é uma identificação, “Seu documento de identidade diz que você é João da Silva” é uma asserção considerada autenticação da identidade.

Já, autenticar um atributo é provar uma associação entre uma entidade e um atributo (Camp, 2004). Por exemplo, a associação entre uma pintura e um certificado de autenticidade. Em um sistema de identidade esse é, geralmente, um processo de duas etapas: primeiramente, é feita uma autenticação de identidade, seguida pela autenticação da associação entre o atributo e o identificador. Um automóvel é autenticado por uma placa de licenciamento, mas é dito como legítimo por uma base de dados de carros que não estão sendo procurados por motivos legais. Claramente, a verificação da placa do carro pode indicar alguma violação e, ainda assim, falhar na autenticação da identidade se a placa está em um carro de modelo visivelmente diferente daquele indicado na base de dados. Uma pessoa é identificada pela carteira de habilitação e a licença simultaneamente autentica o atributo “direito de dirigir”. Há uma diferença significativa entre identificar uma entidade “Seus documentos indicam que você é João da Silva” e autenticar seus atributos “Sua carteira de habilitação permite que você dirija motos e veículos pesados”.

Podemos definir então, em termos gerais, que a autenticação é utilizada para estabelecer a identidade de alguém. A origem da autenticação se deu com os gregos, que criaram a noção de autêntico ou genuíno. Autenticar ficou assim sendo o ato ou processo de estabelecer a autenticidade de alguma coisa ou alguém. No dicionário, autenticação significa estabelecer uma entidade como válida.

A maneira mais comum de se autenticar é através da informação de nome de usuário e senha. Geralmente, um usuário terá um pseudônimo e uma senha atribuídos após uma cadastro inicial. Uma vez atribuídos, o pseudônimo e senha podem ser utilizados para autenticar o usuário.

Já, autorização é definida como a decisão de permitir uma ação em particular com base em um identificador ou atributo (Camp, 2004), ou ainda para permitir ou negar o acesso a um determinado recurso (Recordon e Reed, 2006). Exemplos incluem a habilidade de uma pessoa de abrir linhas de crédito, ou o direito de um veículo de emergência cruzar o sinal vermelho.

2.3 OpenID

Com base nessas definições foi criado o OpenID, que é um protocolo leve de identidade que vem evoluindo constantemente e recebendo atenção da imprensa. Após as maiores empresas de tecnologia, como Microsoft e o Google, anunciarem que se tornaram Provedores de Identidade, ou seja, as partes autenticadoras do processo de identificação de um usuário, é altamente provável que um usuário já possua uma identidade OpenID, apenas nunca a tenha utilizado. Isso torna o protocolo altamente relevante para o processo de autenticação distribuída.

O protocolo OpenID se classifica como centrado no usuário. Autenticação centrada no usuário é um paradigma recente em gerenciamento de identidade. Nesse paradigma o usuário controla, através de interações, todas as transações entre a parte identificadora (também chamada de Provedor de Identidade) e a parte confiante (também chamada de Consumidor de Identidade). Faz parte do protocolo a interação com o usuário, sendo assim, ações que dependem da aprovação dele, como se cadastrar em um site, não são automatizáveis.

Dada a proliferação de adeptos do protocolo, uma vez que o usuário escolhe o provedor da sua identidade, ou seja, quem a mantém, baseado na sua confiança

em relação ao provedor, e que ele controla todas as interações pode-se dizer que a autenticação é centrada no usuário. Uma vez escolhido o provedor, o processo de autenticação é totalmente aberto e descentralizado, envolvendo apenas o usuário, seu provedor e o consumidor de identidade.

O protocolo OpenID lida com autenticação, ficando a encargo do implementador definir autorização para o usuário. É formada assim a base para uma autenticação baseada no usuário, agora em larga escala. Além da modularidade, simplicidade e arquitetura bem formada, a grande vantagem do protocolo é a centralização do poder de escolha no usuário.

O protocolo OpenID põe em dúvida o controle de um usuário sob um determinado atributo, representado por uma URI ou XRI. e uma vez que a escolha desse identificador é do usuário, ele não só pode optar por diversos tipos de identificadores como pode controlar qual identificador fornecerá para um determinado Consumidor de Informação, podendo assim possuir múltiplas identidades.

Também é escolha do usuário optar por qual Provedor de Identidade utilizar, ou ainda instalar e executar um provedor próprio, em uma das diversas implementações disponíveis. E uma vez que o protocolo especifica que a informação da identidade do usuário pode ser facilmente portátil entre Provedores, não há necessidade para que essa escolha seja onerosa para o usuário, dada a facilidade de trocar de provedor.

O usuário também é livre para escolher quais serviços são oferecidos por seu Identificador, bem como quem é o Provedor que os fornece. Com a segunda versão do protocolo, o usuário não está limitado aos serviços providos pelo seu Provedor de identidade. Pode, assim, adicionar dinamicamente suporte para novos serviços à medida que eles aparecem no mercado, facilidade possível através da utilização de documentos Yadis, descritos mais adiante.

2.4 Histórico do OpenID

Tradicionalmente, as aplicações online utilizam seus próprios sistemas de autenticação, criando ilhas de identidade que demanda do usuário a criação, memorização e manutenção de múltiplas senhas e nomes de usuário (Recordon e Reed, 2006).

Nome de usuário e senha são, tipicamente, duas seqüências de caracteres compostas de letras, dígitos e caracteres especiais. O processo oneroso de manter várias identidades, e conseqüentemente várias senhas, leva os usuários a utilizar métodos que diminuem a segurança do sistema como, por exemplo, anotar em algum lugar a senha ou usar a mesma senha e nome de usuário em todos os lugares.

Para mitigar a situação, foi criado o conceito de protocolos de Single Sign-On, onde o usuário só necessita uma senha e só precisa digitá-la uma vez por sessão, como Kerberos e OpenID. Kerberos é comum em ambientes corporativos, mas sua exigência de controle sobre a identidade o torna irrelevante quando se pensa em sistemas controlados por corporações diferentes.

Sendo assim, o protocolo OpenID foi originalmente desenvolvido para fornecer a possibilidade de single sign-on para aplicações web. Concebido em maio de 2005 por Brad Fitzpatrick, atualmente é utilizado em larga escala por usuários do mundo inteiro, que podem desfrutar da praticidade e consistência do serviço.

Fitzpatrick foi também o criador do sistema LiveJournal, e conseqüentemente o suporte ao protocolo foi primeiro implementado nesse serviço. Ao final de junho de 2005, usuários e desenvolvedores do OpenID iniciaram uma colaboração que levaram à criação de dois novos protocolos: LID e Yadis, discutidos mais adiante.

No início de 2007 começaram a surgir as primeiras extensões do protocolo, que suportavam, além de autenticação, a troca de informações de perfil do usuário. Logo em seguida, foi proposto pela comunidade uma maneira de formalizar extensões, e estabelecer um mecanismo para facilitar a sua criação e uso. Ainda nesse ano foi tomada a decisão de estender o protocolo para que permitisse o uso de um identificador compartilhado por múltiplas identidades, tornando o protocolo OpenID um arcabouço de identidade digital, e não só um sistema de autenticação (Wikipedia, 2009).

À medida que a quantidade de usuários foi progressivamente aumentando, também foi a necessidade para novas funcionalidades além da autenticação, foco original do protocolo. Uma comunidade de indivíduos e companhias compartilhavam uma visão onde o OpenID seria um arcabouço onde múltiplas tecnologias correlacionadas poderiam existir. A colaboração dessas partes definiu o que se

tornaria a segunda versão do protocolo, e também especificações auxiliares que ajudariam a estabelecer o protocolo OpenID (Recordon e Reed, 2006).

A idéia original era manter o protocolo OpenID aberto e livre, para que nenhuma empresa controlasse sozinha a especificação. Isso criou uma comunidade forte que ajudou a amadurecer a especificação, desenvolver múltiplas implementações abertas em diversas linguagens e fazer crescer o número de consumidores de identidade, seja como serviço ou como website. Essa metodologia é similar ao esforço que ultimamente resultou no Linux e no Apache, ambos dirigidos por uma comunidade, porém com uma fundação como suporte. Segundo Cameron, a idéia central sempre foi a de que o usuário deve ser o dono da própria identidade, e possuir controle sobre os dados nela contidos e quem a acessa (Cameron, 2005).

2.5 OpenID 2.0

A segunda versão do protocolo foi totalmente estabelecida pela comunidade, sendo completamente compatível com a primeira versão. Assim, novas funcionalidades foram adicionadas sem necessidade de modificação de clientes legados. Adicionou-se um protocolo de transferência de dados, com suporte para uso e atualização de informação. Também foram adicionadas extensões para troca de informações detalhadas da identidade do usuário, bem como suporte para troca de mensagens entre usuários de provedores diferentes.

O objetivo principal foi criar um arcabouço que considera a necessidade de flexibilidade e adaptabilidade pelos provedores com a simplicidade e praticidade dos terceiros que viriam a utilizar o protocolo, visando assim a possibilidade de adoção em larga escala. O protocolo original foi modificado para incluir capacidades antes não possíveis, e permitir não só autenticação, como também reputação, controle de acesso a informações e atualização de informações por terceiros.

2.5.1 Visão geral da arquitetura do protocolo



Figura 1: Stack do Protocolo OpenID

A figura 1 representa o modelo geral de arquitetura em que diferentes tecnologias e protocolos interagem para a formação do modelo completo do OpenID 2.0. URLs e XRIs são os elementos de responsabilidade do usuário, cimentando a base da identidade no mesmo, visto que cabe ao usuário, através de uma URL ou XRI, informar quem provê a autenticação da identidade requisitada. Devido à multiplicidade de protocolos, todos baseados em URL ou XRI, foi criada uma especificação paralela, chamada Yadis que provê informação sobre o protocolo que deve ser automaticamente utilizado.

A camada de autenticação do OpenID fornece o sign-on, base para os outros serviços, impossibilitando a troca de informação sobre a identidade do usuário a não ser que ele seja quem diz ser. Por último, o protocolo de transporte de dados facilita a troca de dados para camadas superiores que dependem de autenticação.

No topo da pirâmide são disponibilizados serviços de alta ordem, como troca de mensagens e informações de perfil, e dependem de implementação específica.

2.5.2 A primeira camada: Identificadores

O termo gerência de identidade centrada no usuário significa uma infraestrutura de identidade digital em que um usuário final tem controle total sobre a disseminação e o uso dos seus identificadores e informações pessoais, também conhecidas como perfil (Recordon e Fitzpatrick, 2006). Para se alcançar tal meta duas metodologias foram utilizadas durante a criação do protocolo:

Identidade baseada em endereços, que utiliza um endereço digital único para identificar o usuário, tanto de maneira pública quanto privada, em um contexto de

uma troca de informação de perfil. Esse endereço é seguido e derreferenciado para descobrir e invocar múltiplos serviços relacionados à identidade do usuário.

Identidade baseada em cartões, que utilizam um token, ou chave, que contém, ou referencia, uma coleção de atributos ou informações que, individualmente ou coletivamente, identificam o usuário e provêm a informação necessária para efetuar transações baseadas em identidade, ou seja, que necessitam de autenticação.

Ambas as metodologias possuem pontos válidos e casos onde são melhores aplicáveis, não sendo contraditórias, uma vez que se pode utilizar um endereço para se descobrir ou requisitar um cartão que, por sua vez, pode referenciar itens através de endereços.

Para oferecer suporte ao descobrimento de serviços e a troca bidirecional de informações, o protocolo OpenID é primariamente baseados em endereços. Usuários são identificados através de um endereço digital em qualquer um dos formatos: URL e XRI. URLs, originalmente especificados no RFC 1738 (Berners-Lee, Masinter *et al.*, 1994), são baseados em IP ou serviços de DNS e são suportados de maneira ubíqua na web, mas seu uso como endereço de identificação digital é relativamente raro.

Como os primeiros utilizadores do protocolo OpenID foram serviços de blogs, considerou-se uma pratica comum representar um usuário pela URL do seu blog. Como é certo que URLs podem representar usuários em outros contextos, XRIs provêm uma maneira consistente, independente de protocolo e segura de endereçamento de usuários (Reed e Mcalpin, 2005). XRIs também suportam IP e DNS, mas são baseados em um prefixo chamado de Símbolo de Contexto Global, representado pelo caractere igual ('='). Esse símbolo foi designado para uso exclusivo de indivíduos. A organização pública e sem fins lucrativos chamada XDI.org é responsável pelo registro de serviços baseados no símbolo de contexto global.

2.5.3 A segunda camada: Descobrimto de serviços

Uma vez que o usuário informa um endereço digital OpenID, o próximo passo é descobrir quais serviços estão associados a essa identidade. Esse é o papel principal do protocolo Yadis (Miller, 2006) para URLs e do protocolo XRI Resolution

para XRIs (Cantor, 2005). Ambos os protocolos são baseados no formato XRDS (Extensible Resource Description Sequence), formalmente especificado pelo comitê OASIS XRI. Há planos para que o protocolo Yadis seja incorporado dentro do XRI Resolution 2.0, consolidando ambas as formas de endereçamento e garantindo que um único protocolo irá reger o descobrimento de serviços tanto baseados em URLs quanto em XRIs.

O processo de descobrimento é simples, e se dá através da execução de um GET protocolo HTTP ou HTTPS em um documento XRDS descrevendo os serviços disponíveis para um endereço em particular. Devido à sua flexibilidade, o protocolo Yadis permite o descobrimento de qualquer serviço, não só aqueles relacionados à identidade.

O propósito de documentos XRDS é listar os serviços disponíveis para uma URL ou XRI. Entretanto, esses documentos também podem conter metadados adicionais sobre controle de cache e associação de identidades (sinônimos).

2.5.4 A terceira camada: Autenticação

O protocolo de autenticação OpenID Authentication é um serviço que permite a um usuário provar que detém o controle sobre uma URL ou XRI i-name. Ele assim o faz através de uma série de mensagens que transitam entre o website no qual o usuário está autenticando (o denominado Consumidor de Identidade) e o provedor de identidade de escolha do usuário (denominado Provedor de identidade).

Primeiramente, o Consumidor de Identidade recebe do usuário a URI, conforme ilustrado na figura 2, e utiliza o serviço de descobrimento para obter a URI do serviço de autenticação. Com o uso de URLs e XRIs como identificadores, o protocolo pode funcionar de maneira totalmente descentralizada, não havendo uma entidade que controla o acesso ou registro de usuários, consumidores de identidades ou mesmo provedores de identidades. Através da capacidade do protocolo de delegar a identidade, é possível que o usuário preserve o identificador OpenID, mesmo que o provedor de identidade seja trocado.

Na segunda versão do protocolo, é possível que o usuário possua um endereço digital privado, um que não o identifica publicamente, mas sim, apenas com um consumidor de identidades, apenas entrando com a URL ou XRI i-name do provedor de identidades. Nesse caso de uso, o consumidor de identidade ainda usa

o protocolo Yadis para determinar o endereço final do serviço de autenticação do OpenID, e começa com o fluxo padrão de autenticação, mas o provedor de identidade reconhece seu próprio endereço digital e pode fornecer ao usuário a oportunidade de enviar ao consumidor de identidade um endereço digital especial, privado. Em uma implementação ideal, o provedor de identidade daria ao usuário final a chance de escolher entre usar seu identificador público ou utilizar um privado.

2.5.5 A quarta camada: Transporte de dados

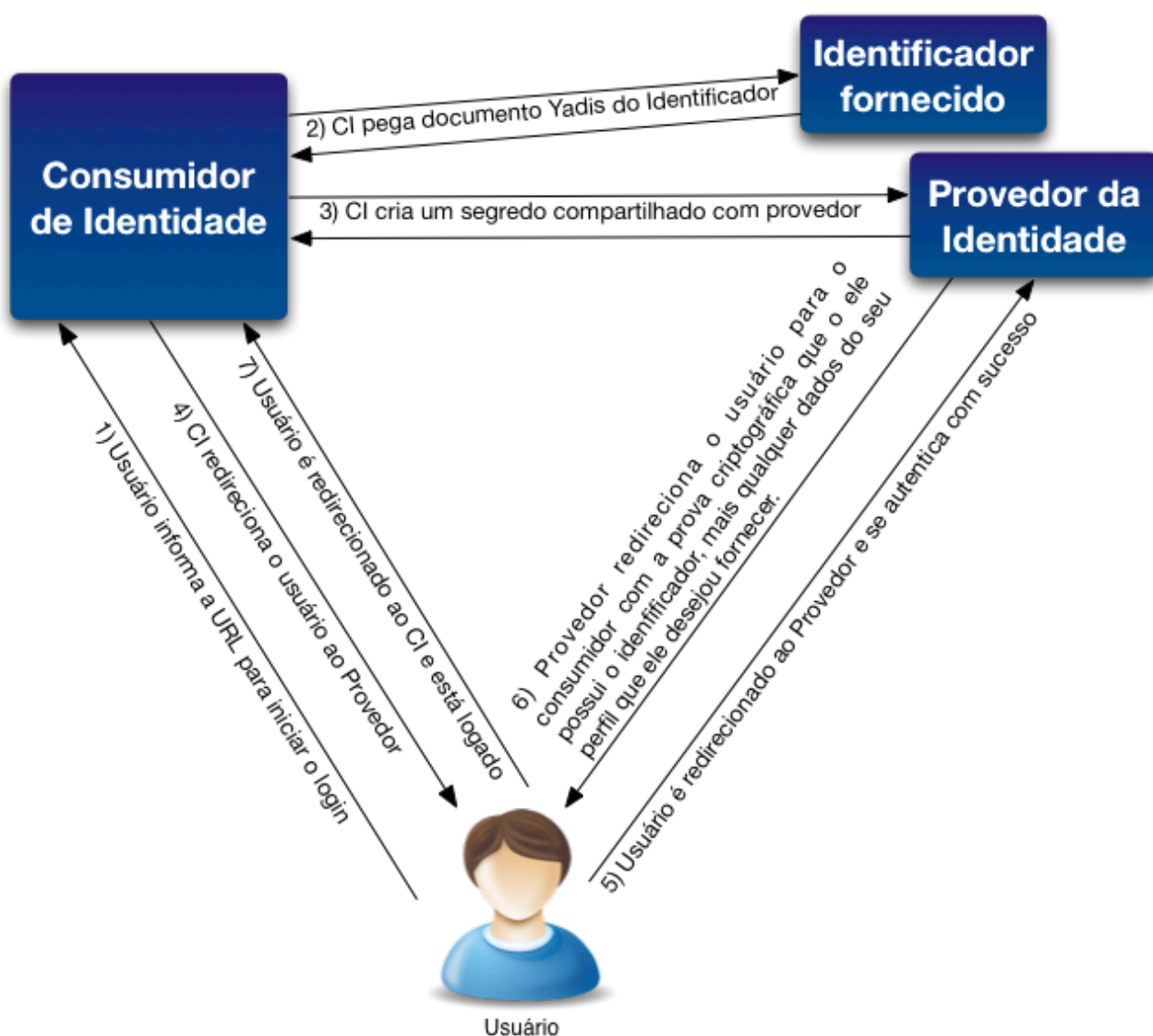


Figura 2: Fluxo básico da autenticação no protocolo OpenID

Com o objetivo de criar pequenas e interoperáveis especificações, o protocolo emergente, denominado OpenID Data Transport Protocol, provê uma abstração para a troca de dados entre Provedores e Consumidores de Identidade. Ele suporta o

fornecimento de informação de perfil entre o Provedor e o Consumidor de Identidade. Ao definir um protocolo abstrato de troca de dados, pode ser que o protocolo OpenID não fique limitado a troca de informações sobre identidade, mas sim, vir a se tornar um arcabouço capaz de suportar troca segura de mensagens, sincronização de dados e outros serviços que requerem a troca de dados autenticados e seguros.

Com o foco específico em troca de informações pessoais, ou perfil, os melhores formatos conhecidos atualmente são definidos pelo OASIS SAML (Cantor, 2005) e pelo projeto Liberty Alliance Project. Ao desacoplar o formato do método de troca, múltiplos formatos, que servem a múltiplos propósitos, podem surgir a partir da comunidade e do mercado.

Um protocolo emergente é o OpenID Attribute Exchange (Hardt, 2006) que provê uma camada de troca de atributos do perfil de um usuário diretamente em uma requisição de autenticação, ou ainda, via DTP. A grande vantagem é a ausência de uma requisição extra, uma vez que, quando o usuário for autenticado, os dados que já estarão disponíveis para os consumidores de informação. Esse protocolo também descreve como Consumidores de Identidade podem requisitar a persistência de dados de perfil diretamente no Provedor de Identidade, provendo uma troca bidirecional de informação.

Em sumo, o arcabouço OpenID tenta solucionar o processo de transporte e troca de dados de maneira aberta e multifacetada. O protocolo *OpenID Data Transport* provê um método robusto para transporte de informação ponto-a-ponto, quando desacoplado do sistema de autenticação, cobrindo os casos de troca de mensagens e sincronização. Já, o protocolo *OpenID Attribute Exchange* provê um método de inserir dados do perfil do usuário diretamente na requisição de autenticação, para que o usuário possa ver e entender exatamente quais informações estão sendo solicitadas pelo consumidor de informação.

2.6 Exemplo de Fluxo do Protocolo OpenID

De acordo com o fluxo normal do protocolo OpenID 2.0, o usuário deve entrar com uma URI de que ele diz possuir controle. Para auxiliar o usuário é comum que os sistemas apresentem múltiplas facilidades para o usuário, como por exemplo,

mostrar o nome e o logo dos maiores provedores de identidade em atividade, para que o usuário possa saber se já possui uma URI OpenID, mas ainda não sabe.

No exemplo a seguir foi utiliza-se o Yahoo como Provedor OpenID. Nesse caso específico, a URL é formada pelo endereço padrão <http://me.yahoo.com/> seguido pelo nome de usuário. No caso do teste foi o usuário `eduardofelipe87`.



Figura 3 - Fornecimento do identificador

Uma vez pressionado o botão de login, o usuário é redirecionado ao site controlado pelo Provedor de Identidade referenciado na URI, como demonstrado na figura 4 a seguir:

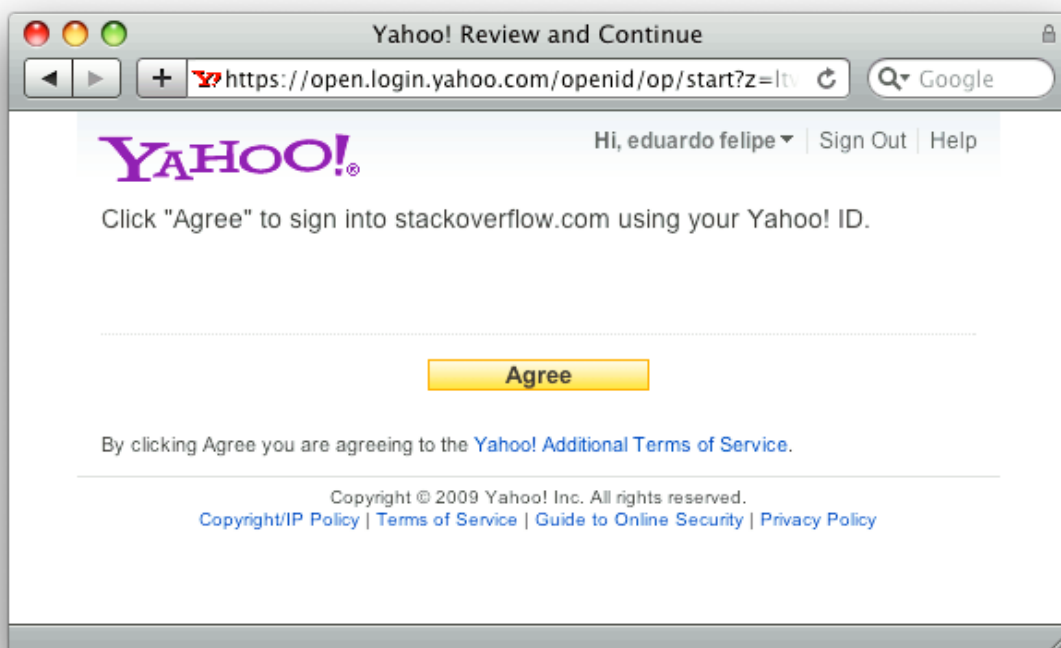


Figura 4 - Aceitando fornecer identificador

Como evidenciado na URL visível no topo da página, o usuário está agora no site do provedor de identidade, que está solicitando ao usuário que permita, ou não, a sua autenticação pela parte confiante. Também é facilmente identificável o nome da parte confiante, nesse caso, o site stackoverflow.com.

Caso o usuário aceite, ele será novamente redirecionado para a parte confiante, agora já autenticado:

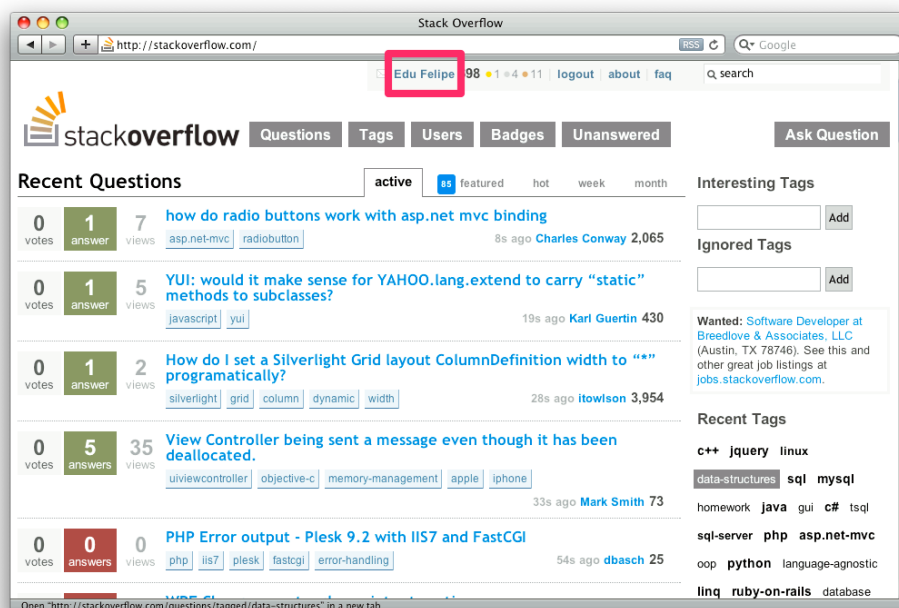


Figura 5 - Verificando login

Caso a parte confiante tenha solicitado alguma informação extra, via Attribute Exchange, isso também é informado ao usuário na figura 6:

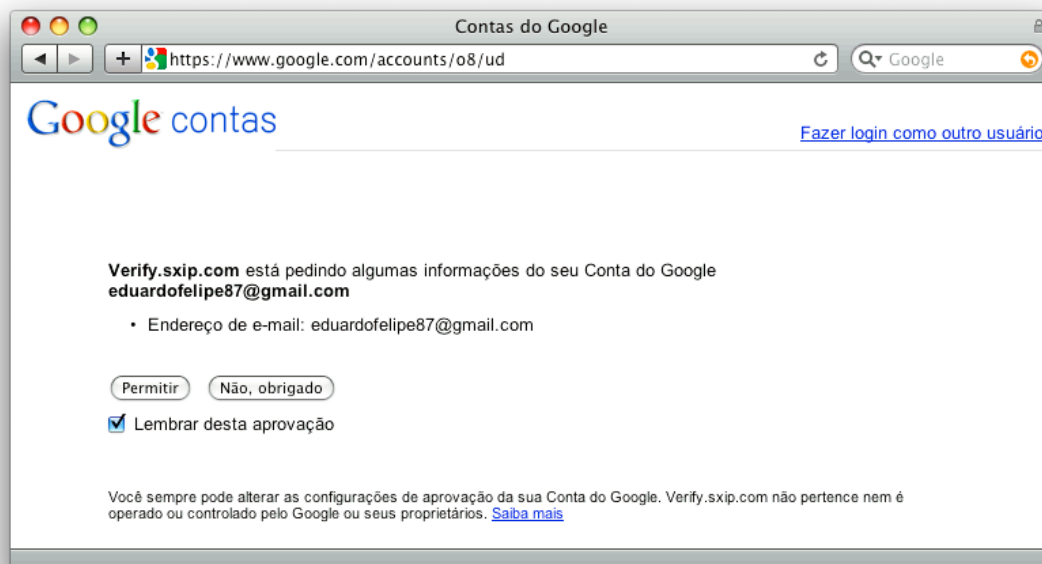


Figura 6 - Permitindo o fornecimento de atributos

2.7 Problemas com o protocolo

Apesar de praticamente todo mundo possuir uma identidade OpenID ela ainda é pouco difundida, uma vez que as grandes empresas são apenas provedores, e não consumidores, de identidade. Sendo assim, são poucos os sites de terceiros que aceitam atualmente uma identificador OpenID como login.

Há também o fato que o processo de autenticação pode ser confuso para usuários inexperientes, já que o redirecionamento dos serviços causa um rompimento na linha de raciocínio do usuário e tem uma confusa mensagem de erro caso o login não tenha sido bem sucedido. Não só isso, mas problemas de segurança ainda não foram solucionados. Como a autenticação é delegada a um terceiro é possível que o usuário sofra ataques de Phishing que acabem comprometendo a integridade da sua identidade.

3 Yadis

Devido à profusão de protocolos para troca de informações baseadas em *URIs* e *iNames* houve a necessidade da criação de um protocolo que possibilitasse

a descoberta de serviços de maneira automática, bem como sua seleção, priorização e utilização de maneira simples e transparente para o usuário.

Caso o usuário forneça apenas uma URL é difícil determinar que protocolos precisam ser usados para identificá-lo e autenticá-lo. Tanto OpenID como OAuth ou LID têm estruturas similares e podem estar relacionados a uma mesma URL. Yadis é um sistema de descoberta de serviços que permite que consumidores de identidade determinem, de maneira automática e sem intervenção do usuário final, qual é o protocolo mais apropriado para utilização.

A especificação do Yadis provê:

- * Um identificador de uso geral para uma pessoa ou entidade, que pode ser usado para todos os serviços anunciados;
- * Uma sintaxe para o documento de descrição de recursos, que identifica os serviços disponíveis usando aquele identificador, bem como a semântica dos elementos desse documento; e
- * Um protocolo para a obtenção do documento de descrição, dado um identificador válido.

Juntas, essas três partes permitem a coexistência e a interoperabilidade de uma multitude de serviços usando o mesmo identificador. O identificador usa uma sintaxe padrão e um namespace bem estabelecido, não requerendo nenhum namespace adicional, bem como nenhuma infra-estrutura administrativa específica.

É importante mencionar que, quando originalmente especificado, o protocolo foi feito para ser usado não só por pessoas ou outras entidades, como empresas e governos, mas também para identificar agentes dessas entidades, como tags de RFID e processos que são executados por um software. Em suma, o protocolo Yadis foi feito para ser usado por qualquer agente de software que deseja descobrir serviços para um identificador, também chamado Yadis ID. Esse identificador, costumeiramente, é uma URL que é informada pelo usuário.

Quando originalmente criado, o protocolo previa apenas a troca de informação sobre serviços de autenticação do usuário. Na sua versão 1.0 foi ampliado para que possam ser anunciados qualquer tipo de recurso, como por exemplo LID, que permite a troca de informações sobre o perfil de um usuário. É possível definir prioridades dentro de um documento Yadis, permitindo que múltiplos

serviços do mesmo tipo coexistam. Em caso de conflito no mesmo nível de prioridade, a ordem de declaração é usada para evitar ambigüidade.

3.1 Uma visão geral do protocolo

Como já foi dito, o propósito do protocolo é permitir que um consumidor de identidade obtenha um descritor de recursos para descobrir os serviços disponíveis para um identificador.

Quando um usuário, ou entidade, oferece um Yadis ID para um consumidor de identidade, esse consumidor de identidade vai querer descobrir os serviços disponíveis naquele Yadis ID.

Para fazer isso, o consumidor de identidade faz uma requisição HTTP. Essa requisição pode ter qualquer uma das seguintes formas:

1. `HTTP GET`: Nesse caso, a resposta da requisição deve conter, em seu cabeçalho HTTP ou dentro do corpo da resposta, que deve ser um documento HTML, a URL contendo a localização do documento Yadis;
2. `HTTP HEAD`: Nesse caso, a requisição deve ser um cabeçalho HTTP contendo a URL com a localização do documento Yadis e o corpo deve ser vazio; e
3. `HTTP GET` e conter no seu cabeçalho uma cláusula `Accept` que indique que ele aceita respostas do tipo documento Yadis: nesse caso, a resposta pode ser o próprio documento, ao invés do documento HTML.

Assim, a resposta de um dos pedidos pode ser:

1. Um documento HTML com um elemento `<head>` que inclua um elemento `<meta>` com o atributo `http-equiv='X-XRDS-Location'`;
2. Uma resposta HTTP que inclua em seus cabeçalhos o cabeçalho `X-XRDS-Location`, em conjunto com um documento;
3. Uma resposta HTTP que inclua apenas cabeçalhos, que deve incluir, além do cabeçalho `X-XRDS-Location` também a especificação MIME de `application/xrds+xml`; e
4. Um documento com o MIME `application/xrds+xml`.

Em todos os casos, o cabeçalho `X-XRDS-Location` deve, obrigatoriamente, apontar para o documento Yadis. Caso esse cabeçalho não exista, será verificado dentro do HTML como `http-equiv`. Caso não exista, e o MIME foi servido como

`application/xrds+xml`, esse documento pode ser considerado como o próprio documento Yadis. Caso contrário, se também não existir esse cabeçalho, a descoberta do serviço é considerada como falha.

Em suma, a resposta pode tanto ser um documento Yadis ou uma URL que localiza esse documento. Caso seja obtida uma URL, o consumidor pode então fazer uma nova requisição nesta URL para obter o documento.

Uma vez seguida uma das alternativas acima listadas, o consumidor deverá ter obtido um documento Yadis originalmente ligado à URL informada pela entidade.

3.2 Formato do documento Yadis

Durante o processo de especificação do Yadis foi considerado-se a possibilidade de oferecer dois formatos de resposta: Um formato em texto puro e outro baseado em XML, tentando facilitar ao máximo aos consumidores de identidade o uso da descoberta de serviços através de URLs YADIS (Miller, 2006).

Entretanto, após estudo foi visto que especificar tanto formato de texto puro quanto um formato baseado em XML proferia pouco valor agregado. Por outro lado usar exclusivamente um formato baseado em XML permitiria o uso de ferramentas já estabelecidas e disponíveis em praticamente todas as linguagens existentes, bem como permitiria incluir informações em futuras versões do protocolo sem que essas informações invalidassem ferramentas construídas para versões anteriores do protocolo.

Com essa decisão o documento Yadis especificado é baseado em um formato XML simples e extensível chamado *Extensible Resource Descriptor* (Descritor de recursos extensível, tradução nossa) ou ainda abreviado como XRD. O formato de documentos XRD é especificado pelo comitê técnico do OASIS (Cantor, 2005). É possível achar na especificação do Yadis o esquema XML criado para documentos Yadis, que permite a geração automática de ferramentas para descodificação desse tipo de documento.

O documento Yadis contém um descritor de recursos Yadis, que possui uma lista de identificadores para todos os serviços existentes. Esses são os serviços que conhecem o usuário identificado pelo Yadis ID usado para obter o documento Yadis. No caso de alguns serviços, dados adicionais são incluídos no descritor de recurso para que eles sejam usados por um consumidor de identidade ao fazer requisições

para aquele serviço específico. Nesse caso, não é papel do Yadis especificar a sintaxe e semântica dessas informações, mas sim papel do criador da especificação daquele serviço específico.

O descritor de recursos Yadis também permite que o usuário especifique que serviços são de sua preferência.

Um exemplo simples de documento Yadis é apresentado abaixo:

```
<?xml version="1.0" encoding="UTF-8"?>
<xrds:XRDS
  xmlns:xrds="xri://$xrds"
  xmlns="xri://$xrd*($v*2.0)">
  <XRD>
    <Service priority="1">
      <Type>http://specs.openid.net/auth/2.0/server</Type>
      <URI>http://example.com/server/endpoint/</URI>
    </Service>
    <Service>
      <Type>http://lid.netmesh.org/sso/2.0 </Type>
    </Service>
  </XRD>
</xrds:XRDS>
```

Esse documento de exemplo fornece dois serviços, de tipos diferentes, um do tipo OpenID 2.0 e outro do tipo LID 2.0.

Obrigatoriamente, todos os serviços oferecidos devem estar dentro do namespace da tag `<XRD>` uma vez que são sujeitos à especificação feita pela OASIS. Como esse elemento é considerado o elemento raiz do documento Yadis, caso mais de um esteja presente, será considerado apenas o último (Reed e Mcalpin, 2005).

Dentro do namespace XRD devem existir um ou mais elementos do tipo `<Service>` que descrevem um serviço. A ordem dos serviços não é significativa a não ser quando há conflito de prioridades. Nesse caso, o serviço a ser escolhido é dependente da implementação, com o caso comum sendo por ordem de declaração.

Cada elemento `<Service>` pode, opcionalmente, ter o atributo `priority` com valor numérico. O objetivo desse atributo é permitir ao usuário dizer qual dos serviços devem ser usados caso haja múltiplos serviços do mesmo tipo sendo anunciados. A preferência é dada primariamente para o serviço com o menor valor

de `priority`, depois àqueles que possuem valor mais alto e por último àqueles que não possuem valor algum explicitamente designado para o atributo (Wachob, 2005).

Cada serviço deve conter um elemento `<Type>` que indica o seu tipo. Caso um serviço não contenha tipo, ele não é considerado um serviço válido. Esse elemento deve conter o endereço que aponta para a especificação que rege o serviço que está sendo descrito. Em geral, ele tende a ser uma URL que é acessível por qualquer browser e que contém uma cópia da RFC daquele serviço. Também é comum que essa URL contenha a versão do documento, para que possa ser usada para evitar ambigüidade (Miller, 2006).

Por último, os elementos do tipo `<Service>` podem conter elementos do tipo `<URI>` que devem apontar para o recurso que provê o serviço. Caso haja mais de um elemento `<URI>` eles são considerados equivalentes, e podem ou não ser tentados em série pelo consumidor de identidade. Eles também podem ter prioridade, com a mesma semântica da prioridade do elemento `<Service>`. A prioridade permite uma flexibilidade grande, visto que não há a necessidade do documento Yadis e o serviço final estarem dentro do mesmo domínio. Isso pode ser usado para implementar delegação de serviços. O serviço de OpenID possui uma outra sintaxe para delegação, que será vista a seguir.

Como já foi citado, dentro do elemento `<Service>` é permitida a existência de outros elementos com informações específicas a um serviço. Abaixo há um exemplo de um documento Yadis que demonstra essa possibilidade:

```

<?xml version="1.0" encoding="UTF-8"?>
<xrds:XRDS
  xmlns:xrds="xri://$xrds"
  xmlns="xri://$xrd*($v*2.0)"
  xmlns:openid="http://openid.net/xmlns/1.0">
  <XRD>
    <Service priority="0">
      <Type>http://specs.openid.net/auth/2.0/server</Type>
      <URI>http://example.com/server/endpoint/</URI>
      <openid:Delegate>
        http://smoker.myopenid.com/
      </openid:Delegate>
    </Service>
    <Service>
      <Type>http://lid.netmesh.org/sso/2.0 </Type>
    </Service>
  </XRD>
</xrds:XRDS>

```

Como se pode observar, o documento adiciona um novo namespace de XML, chamado `openid`, e usa um elemento desse namespace `<openid:Delegate>`. Esse caso também demonstra como deve ser efetivada a delegação de autenticação do OpenID através de documentos Yadis. Uma vez que essa semântica é exclusiva do OpenID, fica a encargo dos autores do protocolo especificar elementos extras.

4 Reputação Digital

Sistemas de reputação online são uma maneira de baixo custo de coletar e agregar feedback sobre os usuários de um determinado sistema. Esses sistemas, também conhecidos como sistemas de pontuação ou feedback, são uma tentativa de se reestabelecer o papel da informação interpessoal, também conhecida como boca-a-boca, em sistemas online. Essa informação tem como propósito sinalizar qualidade e induzir comportamentos positivos na presença de assimetria de informação sobre a identidade dos componentes de um grupo (Resnick, Kuwabara *et al.*, 2000).

Esses sistemas agregam a opinião dos membros de uma comunidade online sobre experiências prévias com outros membros dessa mesma comunidade. Quando um membro fornece sua opinião sobre outro membro, essa opinião é agregada e normalizada com a opinião de outras partes dessa comunidade e acaba por formar a reputação de um indivíduo dentro da comunidade.

Múltiplos exemplos de tais mecanismos já estão sendo utilizados por comunidades estabelecidas, como eBay, por exemplo, que depende exclusivamente do seu sistema de reputação para criar confiança e induzir bom comportamento nos seus integrantes. Compradores e vendedores do eBay são altamente encorajados a registrar suas opiniões sobre a outra parte envolvida em todas as transações ocorridas. Possíveis valores para a qualidade de uma transação são “boa”, “ruim” ou “neutra”, sempre seguidas de um curto comentário textual sobre o usuário. O eBay faz a soma total de todas as avaliações de seus membros, bem como os comentários individuais das transações, disponíveis para todos os usuários registrados. Um corpo crescente de estudos indica que o sistema de reputação do eBay provê estabilidade e segurança consideráveis em um ambiente que, sem reputação, seria arriscado (Houser e Wooders; Lucking-Reiley, Bryan *et al.*, 1999; Bajari e Hortacsu, 2000; Dewan e Hsu, 2004).

É crescente a importância de sistemas de reputação online para participantes de comunidades, não só de comércio eletrônico mas também comunidades de software livre. Ainda assim necessitam de pesquisas mais rigorosas sobre seu funcionamento e eficácia. Questões tais como até que ponto eles podem ser manipulados por membros estrategistas que desejam obter reputação apenas para adquirir a capacidade de danificar a comunidade no futuro.

4.1 O que é reputação

Os conceitos de reputação e redes de troca de informação interpessoal, também conhecidas como boca-a-boca, são tão velhas como a própria sociedade. Muito antes de um estabelecimento formal de lei e desenvolvimento de sistemas contratuais centralizados, auxiliados pelo poder soberano de um Estado, comunidades primitivas e medievais dependiam de reputação como o facilitador principal de atividades econômicas e sociais (Milgrom, North *et al.*, 1990).

Enquanto em sociedades a reputação de um indivíduo baseado em boca-a-boca usualmente emerge de maneira natural, sistemas de reputação on-line tentam induzir artificialmente as dinâmicas do sistema tradicional no cyberspaço através do uso de tecnologias da informação. A análise e o projeto, quando bem executados, exigem um profundo entendimento de como os efeitos da reputação ocorre naturalmente em situações sociais.

De acordo com Wilson (1995), reputação é a característica ou atributo designado a uma pessoa (organização, comunidade, etc.) A por outra pessoa (ou comunidade) B. Operacionalmente, isso é comumente expressado como uma previsão sobre o provável futuro comportamento de A (“A provavelmente será justo”). Entretanto, é primariamente uma asserção empírica sumariando observações sobre atos passados de A, sob a ótica de B (“B diz que A foi justo com ela no passado”). O poder da reputação na interação social é baseado na premissa de que um comportamento anterior é um bom indicativo para um comportamento futuro.

Nos últimos vinte anos, economistas tentam aplicar a semântica da teoria dos jogos em situações reais. A idéia principal é que a reputação é uma variável de estado que depende da observação das ações passadas de um indivíduo por outro e que afeta as possíveis recompensas do indivíduo observado.

Podemos tomar, como um exemplo concreto, sistemas de agregação de críticas sobre filmes, como Metacritics ou Rotten Tomatoes, conhecidos pela avaliação e classificação de filmes em uma escala numérica. Eles agregam e normalizam as notas de críticos e usuários que já assistiram um determinado filme; na prática, resumindo o passado. O poder desses sistemas está na habilidade de influenciar a crença de determinados indivíduos sobre o quanto eles gostarão de um determinado filme, influenciando na a decisão de assistir ou não o filme em questão.

De maneira geral, a reputação é importante em cenários onde:

- Há múltiplos indivíduos;
- Pelo menos um dos indivíduos possui alguma informação privada que persiste ao longo do tempo; e
- De um indivíduo informado é esperado a execução de uma série de ações e o mesmo é impossibilitado de se comprometer de maneira crédula antes das ações serem efetivamente executadas.

Em tal cenário, as futuras ações de indivíduos desinformados dependem nas suas crenças das informações privadas do indivíduo informado. Caso haja um sinal observável, que correlacione com as ações do indivíduo informado e podem revelar alguma coisa útil sobre suas informações pessoais, então esse sinal pode ser utilizado para atualizar as crenças do indivíduo desinformado e conseqüentemente sobre o seu futuro comportamento em relação ao indivíduo informado. Assim ,reputação cria uma ligação temporal ao longo de uma seqüência de ações

discretas: quando estiver escolhendo sua próxima ação, o jogador informado deve levar em consideração não só a recompensa a curto prazo, mas também as consequências a longo prazo das suas ações baseado em o que aquela ação revela sobre suas informações pessoais para os outros indivíduos.

O fator crucial que distingue reputação de outras maneiras de se estabelecer o resultado de interações sociais é a falta de comprometimento digno de crédito, geralmente de todas as partes envolvidas na interação: Se um vendedor pode, de maneira digna de crédito, se pré-comprometer a apenas oferecer bens de qualidade, ou ainda, se um vendedor pode se comprometer a enviar um vendedor para a prisão caso ele o engane então não há necessidade do vendedor manter uma reputação de honestidade.

A falta de confiança em qualquer forma de comprometimento é a maior vantagem da reputação: cooperação baseada em comprometimento geralmente exige custosas tecnologias para serem executadas de maneira justa, enquanto que a cooperação baseada em reputação não exige: o principal efeito da reputação é criar em todos os indivíduos uma resposta cooperativa através da maximização dos ganhos futuros individuais. Em contrapartida, a falta de comprometimento torna os efeitos da reputação deveras frágeis e sua análise muito mais complexa. Além disso, o equilíbrio da reputação não se dá sem custo. Na maioria dos casos ela resulta de ineficiências cujo custo precisa ser cuidadosamente calculado e comparado contra os benefícios do não comprometimento.

Finalmente, é importante notar que os efeitos da reputação não necessariamente beneficiam a sociedade. De acordo com o cenário eles podem resultar tanto em um benefício social quanto custarem recursos preciosos a sociedade. Em alguns casos, a reputação pode induzir comportamento cooperativo em ambientes competitivos. Em outros casos, a reputação pode permitir a um indivíduo manipular outros indivíduos para que esses se comportem de uma maneira que melhor o beneficia, mesmo que esse comportamento não seja benéfico para o seu portador.

Como um exemplo clássico tem-se uma versão repetida um finito número de vezes do dilema do prisioneiro (Kreps, Milgrom *et al.*, 1982). Sabe-se que tanto na versão única como na repetida, a estratégia dominante é delatar o outro prisioneiro

em todas as rodadas, mesmo sabendo que o benefício seria maior se eles cooperassem.

A situação muda radicalmente se há alguma dúvida, não importa quão pequena, na concepção de cada prisioneiro sobre o outro. Supondo, por exemplo, que cada prisioneiro acredita que o outro é do tipo retaliador: Alguém que coopera contando que o outro coopere, e que sempre delata o oponente na rodada seguinte a uma que ele foi delatado. Kreps et. al. mostra que, nessa situação, é em benefício próprio a longo prazo manter a reputação de ser retaliador ao cooperar em todas as rodadas a não ser quando for delatado.

Um outro exemplo de sistemas de reputação são chamados estratégias estáveis de comportamento, como o jogo de redes de lojas (Kreps e Wilson, 1999). Na versão mais simples uma empresa, denominada de “dominante”, joga em seqüência contra outras empresas, denominadas “aspirantes”, da seguinte maneira: Cada aspirante escolhe se deseja abrir uma loja próxima a uma loja dominante ou se deseja ficar de fora. Se a aspirante decide ficar de fora ela não recebe nenhuma pontuação. Caso decida abrir a loja, então, a sua pontuação depende da reação da dominante. Se a dominante decidir “lutar” (se engajando em uma guerra de preços) então a aspirante perde um ponto. Se a dominante se “acomodar” e não fizer nada então a aspirante ganha um ponto. Caso a aspirante decida não abrir a loja a dominante recebe dois pontos. Se a aspirante abrir a loja e a dominante se acomodar ela recebe um ponto. Se a dominante decidir lutar, então ela perde um ponto, fazendo com que ambas percam em caso de uma luta. Cada aspirante maximiza a próxima rodada, enquanto a dominante maximiza a soma da sua pontuação ao longo do jogo. Na falta de assimetria de informação é óbvio que o equilíbrio só será atingido caso a aspirante abra a loja e a dominante se acomode em todas as rodadas do jogo: Se acomodar é a estratégia ótima para a loja dominante em todas as rodadas do jogo e abrir a loja é a melhor resposta de todas as aspirantes.

Imaginando que seja injetada uma informação imperfeita no jogo, ou mais especificamente, se assumirmos que na mente da aspirante há uma probabilidade não zero que a dominante é do tipo “forte”, ou seja, que está determinada a lutar não importa qual o custo disso. Kreps e Wilson demonstram que uma dominante “fraca” (o oposto da forte) pode tirar vantagem dessa incerteza para manter a

reputação de “forte” ao imitar o comportamento de uma do tipo “forte”: sempre lutar com aspirantes mesmo que isso cause perdas no curto prazo. Conhecendo esse fato a maior parte das aspirantes não vão tentar abrir lojas, resultando em lucro a longo prazo. O efeito da reputação então permite que uma dominante “fraca” possua todo o mercado, exceto talvez por pequenas aspirantes que se arriscaram.

Em todas as transações, comerciais ou não, em que uma das partes executa a ação (envia um pagamento, envia um produto, concede permissão de administrador, abre uma loja) antes que a outra, há uma exposição à conduta moral de uma das partes. Em tais situações a parte que executa a ação posteriormente tem duas possibilidades, cooperar ou trapacear, com as seguintes propriedades: a ação benéfica para a segunda parte (trapacear) é menos benéfica para a primeira parte, e vice versa. Além disso, a primeira parte envolvida na transação não tem poder direto sobre a escolha da outra parte.

A literatura econômica provê uma série de exemplos de situações em que os efeitos da reputação são percebidos como em (Wilson, 1995).

4.2 A Fragilidade da reputação

O modelo padrão de reputação, apresentado anteriormente como teoria do jogo, torna aparente que reputação é um sistema poderoso, ainda que frágil. A eficácia varia com o tempo. Além disso é freqüentemente dependente de outros parâmetros do meio, geralmente de maneira sutil e inusitada. Finalmente, o equilíbrio da reputação em uma comunidade exige um custo na forma da redução da eficiência. Esse custo deve ser comparado com o custo de alcançar um feito similar através de outras maneiras (como por exemplo, contratando membros da comunidade). O projetista de um sistema de reputação virtual deve ter familiaridade com a volatilidade que a reputação tende a tomar nesses sistemas,

4.2.1 Do dinamismo da reputação

Reputação é uma propriedade altamente sensível à passagem do tempo. Quando um novo membro entra em uma comunidade ele precisa construir sua reputação do zero. Uma vez construída ela precisa ser mantida. Finalmente, quando consideramos comunidades com um objetivo e fim definido, é possível que alguns membros tirem vantagem da reputação adquirida em benefício próprio pouco antes de ser atingido o objetivo da comunidade.

Iniciar um mecanismo de reputação é algo não trivial. Tendo como exemplo o modelo do site de compra e venda eBay, no começo de um ciclo de vida de um novo vendedor, seus possíveis compradores não possuem informações sobre a reputação do vendedor. Para que essa reputação seja criada, em primeiro lugar, alguns compradores devem estar suscetíveis a transacionar com o novo vendedor. Além disso, esses corajosos compradores devem estar dispostos a disseminar a reputação do vendedor na forma de feedback para a comunidade. Não é óbvio o motivo de por quê eles deveriam fazer isso. De maneira mais geral, não é óbvio porque membros de uma comunidade contribuiriam com feedback para um mecanismo de reputação. Na verdade, princípios econômicos básicos prevêm que avaliações, que são bens públicos, são provavelmente subofertadas. Avery, Reskick e Zeckhause (1999) estudaram esse problema e sugerem um mecanismo de ajuste de preços e subsídio que opera em mercados computadorizados e induzem à proliferação de avaliações.

Durante a fase inicial não é incomum que novos membros se sujeitem a ações altruísticas, como reduzir margens de lucro, ou até operar com margens negativas, realizar triagem de problemas na base de problemas ou outros trabalhos não desejados por membros estabelecidos de uma comunidade, enquanto a comunidade “aprende” sobre sua índole. Nesses casos os membros só entrarão na comunidade se o custo da fase inicial, transformado em reputação para fases posteriores, representar algum ganho pela detenção dessa reputação.

Outra consideração é se os incentivos para induzir um bom comportamento por parte da comunidade funcionam corretamente. A resposta, aqui, depende da situação. Na maioria dos casos, o efeito da reputação começa imediatamente e é mais perceptível durante a fase inicial, em que novos membros devem trabalhar arduamente para estabelecer as bases de uma reputação. Holmstrom (1999) discute um modelo interessante de considerações acerca da reputação no contexto da “carreira” de um membro: suponha que a remuneração é uma função da habilidade inata de um funcionário para uma tarefa. Empregadores não podem diretamente observar a habilidade de um empregado. Eles podem, contudo, contabilizar o valor agregado das tarefas já executadas por ele. O valor agregado depende tanto de habilidade quanto de esforço. O objetivo de um empregado é maximizar o seu ganho enquanto minimiza o seu esforço. Em estado de equilíbrio, isso provê incentivos

para que o empregado trabalhe arduamente desde o começo de sua carreira. Esses incentivos são mais fortes logo no começo da carreira, onde observações por parte do empregador são mais informativas.

Em contraste temos Diamond (1989) que, em sua análise da formação da reputação em mercados financeiros, apresenta um cenário em que efeitos da reputação não funcionam logo no começo. No modelo de Diamond há três tipos de investidores: os seguros, que são quem sempre selecionam modalidades de investimento onde a probabilidade de perda é zero; os agressivos, que sempre selecionam modalidades arriscadas, em que os ganhos podem ser altos mas a probabilidade de perda é maior que zero; e os estrategistas, que selecionam o tipo de modalidade que maximiza o ganho a longo termo. O objetivo dos bancos que emprestam os recursos é maximizar o seu retorno a longo prazo ao oferecer uma taxa de juros baixa para os investidores e, ao mesmo tempo, distinguir os investidores lucrativos dos não lucrativos. Os bancos não observam a escolha de modalidade dos seus investidores, mas têm acesso ao histórico de sucesso deles. Nesse estado, a reputação é fundamental. Nesse modelo, se os bancos acreditaram que a fração inicial de investidores agressivos é significativa, então, ao contrario da reputação, no começo do jogo taxas de juros vão ser tão altas que investidores estrategistas têm um incentivo para agir agressivamente. Alguns deles vão perder e sair do jogo. Outros vão se provar lucrativos e ser considerados como seguros. É apenas depois que investidores estrategistas que tiveram sorte de terem adquirido uma reputação inicial, e conseqüentemente uma taxa de juros mais baixa, que se torna um comportamento ótimo para eles agir como investidores seguros afim de manter sua boa reputação.

Modelos de reputação são geralmente caracterizados por um estado intermediário, denominado de estado de equilíbrio, em que o estado da variável interpretada como “reputação” alcança um valor e permanece estável através do tempo. A questão mais importante é se esse estado de fato existe na prática. Uma alternativa seria uma situação em que o vendedor acha o balanço ideal entre manter uma reputação e tirar proveito dela. Segundo Dellarocas (2001a) se a oscilação na reputação for ótima, o valor real do mecanismo da reputação seria diminuído significativamente. Shapiro (1982) estudou esse problema e chegou a um conjunto de condições primordiais para a existência do estado de equilíbrio.

Considerando que reputação é geralmente baseada na observação imperfeita das ações de um indivíduo, outra consideração importante nesse estágio é se o objetivo de manter a reputação de um indivíduo em um nível estável é suficiente para induzir outros membros de uma comunidade a se comportarem bem.

Mais uma vez, a resposta depende dos detalhes exatos sobre que variável é interpretada como reputação e como ela muda com o passar do tempo. É interessante notar que, no caso mais comumente encontrado na prática, que é basear a reputação na média de todas as observações passadas do comportamento de um indivíduo, a resposta para a pergunta acima é um claro não. Quanto mais um jogador permanece no jogo, menor é o efeito de suas ações atuais sobre a sua reputação média. Então, de maneira contra intuitiva, jogadores que jogam há muito tempo têm um incentivo menor para se comportar adequadamente que novos jogadores. Esse fenômeno foi descoberto por Holmstrom (1982) na sua análise de um modelo de carreiras: O modelo dele prevê que, no equilíbrio, empregados têm menos incentivos para trabalhar arduamente em estágios tardios da sua carreira que logo no começo. Uma vez estabelecida uma boa reputação, expressada como média do valor agregado da sua produção ao longo de toda a carreira, continua com eles mesmo que o valor agregado caia. A implicação desse fenômeno para mecanismos de reputação online é clara: deve-se substituir médias simples por médias ponderadas que dão proporcionalmente mais importância ao feedback recente.

Uma das limitações de usar reputação para induzir um bom comportamento é que os efeitos da reputação só funcionam se o jogador pretende permanecer no jogo por um longo tempo. Como já foi discutido, logo que o jogador deseja sair do jogo o custo de manter uma reputação excede o benefício associado a exploração do jogo, conseqüentemente o vendedor encontra a solução ótima ao começar a trapacear com crescente probabilidade.

Uma das possíveis soluções para esse problema é acrescentar algum valor para a reputação uma vez que o jogador não mais esteja interessado no jogo, para que eles ainda considerem uma vantagem manter a reputação no estágio final da sua saída do jogo. Por exemplo, reputação poderia ser vista como um bem que pode ser vendido e comprado em um mercado de reputações (Tadelis, 2001).

Outra possível solução é exigir um depósito de algum bem de valor para todos os novos membros, depósito esse que só vai ser devolvido quando o jogador sair se ele tiver uma boa reputação. Essa é uma idéia interessante, especialmente em comunidades online, porque ajuda a diminuir os problemas de troca de pseudônimos, visto adiante.

Há também o problema da relação sinal/ruído a ser observada no cálculo da reputação de um indivíduo. Na maioria das situações reais a reputação é derivada de uma observação imperfeita de um sinal. A soma das imperfeições observadas pode, com freqüência, mudar o equilíbrio da reputação e causar uma perda de eficiência. Outros problemas podem surgir quando o sinal usado como feedback é imperfeitamente correlacionado com o comportamento que ele afirma revelar. Nesses casos, jogadores podem ser capazes de, estrategicamente, modificar seu comportamento para gerar um sinal de “boa qualidade” mais ainda esconder sua verdadeira índole. Um exemplo clássico de um estudo baseado em eventos reais vem de Dranove et. al (2003) sobre os efeitos dos relatórios de óbitos médicos, na forma de divulgação do índice de mortalidade de médicos e hospitais. O propósito desses relatórios era informar o público em geral sobre a eficácia de hospitais e médicos e prover incentivos para que aqueles com altas taxas de mortalidade possam melhorar a sua eficácia. Estudos iniciais em Nova York no final da década de 90 concluíram que esses relatórios ajudaram a reduzir a taxa de mortalidade nos hospitais. Porém, uma inspeção mais detalhada revelou que, logo após a introdução do sistema de relatórios, os hospitais mudaram as políticas de triagem de pacientes, recusando tratamento a pacientes de alto-risco ou terminais. Sendo assim, eles eram capazes de diminuir a taxa de mortalidade sem melhorar a qualidade de atendimento.

4.3 Considerações adicionais sobre reputação online

4.3.1 Pseudônimos

Na maioria das comunidades online a noção de identidade é fraca e local. Membros geralmente se conhecem através dos pseudônimos utilizados, que são difíceis de correlacionar com uma pessoa “real”. Além disso, é possível uma mobilidade de pseudônimo, onde membros de uma comunidade podem trocar de identificador de maneira simples e com custo mínimo (Friedman e Resnick, 2001).

Em tais ambientes, jogadores de longo prazo têm mais uma estratégia disponível: eles podem desaparecer a qualquer momento e reaparecer sob uma nova identidade, e com ela adquirir um histórico limpo. Em alguns casos, isso pode criar uma possibilidade de jogar com o sistema onde, periodicamente, o mesmo usuário entra na comunidade, constrói uma boa reputação, danifica a comunidade em benefício próprio, sai da comunidade e retorna sob uma nova identidade. Sendo assim, é importante levar em consideração essa possibilidade quando se está trabalhando com mecanismos de reputação online.

Friedman e Resnick discutem duas maneiras de se considerar esse problema: Tornar difícil a mudança de identidade online ou estruturar a comunidade de tal maneira que a saída e a reentrada com uma nova identidade não seja vantajoso para quem assim o faz. A primeira maneira faz uso de autenticação criptográfica e forte ligamento entre a reputação e a URI de uma identidade, já a segunda é baseada em criar um custo inicial para a construção de reputação, como por exemplo, limitando a capacidade dos usuários quando sua reputação for abaixo de um nível mínimo. Sendo assim, o custo de recomeçar o processo de escalada de privilégios custa mais do que os possíveis benefícios de se explorar uma comunidade.

4.3.2 Manipulação estratégica de mecanismos de reputação.

À medida que a reputação digital associada a uma identidade começa a exercer uma maior influência no processo de tomada de decisão de uma comunidade, o incentivo para manipulação estratégica da acumulação de reputação começa a crescer. O custo baixo de se fornecer reputação digital, junto com a relativa anonimidade dos indivíduos que julgam os seus pares faz com que a manipulação seja um problema real que precisa ser estudado com cuidado antes que seja possível atingir uma adoção em massa de um sistema de reputação unificado centrado no usuário.

Diversas comunidades que possuem sistemas de reputação tentaram resolver esse problema através do uso de um conceito comumente chamado de “Avalie o avaliador”: membros podem avaliar o quão útil é a avaliação de outros membros e, conseqüentemente, a reputação fornecida por eles foi válida. Embora essa técnica seja válida para a redução da distribuição gratuita de reputação, ela não é efetiva

para reduzir manipulação estratégica. Indivíduos que manipulam o sistema podem também manipular o sistema de “Avalie o avaliador”, inflacionando a reputação em uma comunidade.

Até o momento há poucos estudos sob a área de manipulação de reputação digital. Dellarocas (2000) apontou uma série de cenários e propôs alguns mecanismos de prevenção de manipulação que reduz os manipuladores a uma fração relativamente pequena (de 20% a 30%) da população total da comunidade. Mayzlin (2006) analisou o impacto da manipulação de reputação em fóruns online, onde a reputação gera apenas uma escalada de privilégios.

Um dos problemas que complicam a remoção da manipulação estratégica de reputação online é a relativa assimetria que existe hoje entre os incentivos dos que são avaliados e o incentivo dos que avaliam. Enquanto um mau comportamento de um avaliado resulta em uma baixa de reputação pelo avaliador que, em consequência, reduz os futuros benefícios do avaliado, na maioria dos sistemas o comportamento desonesto de um avaliador não implica em consequências maiores que simplesmente ter a sua avaliação ignorada. Até em sistemas onde ambas as partes podem se avaliar mutuamente ainda há uma assimetria significativa: Por exemplo no sistema de compra online eBay, onde vendedores também avaliam compradores, uma má avaliação de um comprador não têm efeito algum, já que um vendedor não tem o direito de negar ofertas de compra da parte de maus compradores, enquanto um comprador pode certamente se negar a comprar de um mau vendedor.

Um maior progresso nessa área requer mecanismos que impõem algum tipo de custo para a avaliação desonesta (ou, em contrapartida, beneficia o comportamento honesto). Mas isso, mais uma vez, é sujeito a julgamento moral. Uma vez que não é possível ler a mente dos indivíduos, um comportamento honesto genuíno não pode ser diretamente observado. Em alguns casos, a desonestidade pode ser identificada como desvios estatísticos. Na maioria dos casos, porém, reputação envolve um certo grau de subjetividade: nesses casos, é difícil dizer se um desvio estatístico realmente representa um comportamento desonesto ou uma crença diferente sobre a reputação alheia.

4.4 Alternativas arquiteturas para reputação

Até agora foi presumida uma arquitetura centralizada em que feedback é explicitamente provido e um único mediador controla a agregação e distribuição de reputação. Mesmo que as possibilidades de projeto dessa arquitetura simples não sejam completamente entendidas (Dellarocas, 2001b), modelos centralizados de reputação não oferecem todas as possibilidades disponíveis a sistemas online de reputação.

O estudo de sistemas multi-agente tem focado recentemente em mecanismos de reputação online como uma tecnologia para construir confiança e induzir bom comportamento em sociedades artificiais de agentes em um sistema. Duas linhas de investigação se destacam como promissoras.

4.4.1 Formação de reputação implicitamente

Na nossa sociedade, digitalmente conectada, múltiplos traços das atividades de um agente podem ser encontradas em base de dados acessíveis publicamente. Ao invés de depender de feedback explícito de outros membros, mecanismos automáticos de feedback possuem a capacidade de inferir aspectos de um atributo de um agente, índole e histórico comportamental através da coleta e análise de tais informações implícitas.

A aplicação mais recente atualmente talvez seja exemplificada pelo mecanismo de busca criado pelo Google. Esse mecanismo designa uma medida de reputação para cada página da web que se encaixa em um termo de busca. Ele usa, então, essa medida para ordenar as páginas. O algoritmo de reputação de páginas do Google, chamado de "Page Rank" mede a importância de uma página com base no número de links que apontam para essa página, o número de links que apontam para a página que aponta para a página e assim sucessivamente (Brin e Page, 1998). O conceito base é que se um número suficiente de pessoas considera que uma página é importante o suficiente para criar um link que aponta para aquela página em sua página e, se a sua própria página possui uma reputação boa o suficiente, então a informação contida na página apontada provavelmente é válida. O sucesso desse algoritmo em retornar resultados relevantes é um indicativo da qualidade de reputação que esse tipo de sistema implícito pode gerar.

Pujol et al. (2002) aplica técnicas de fluxo de grafos para sugerir uma generalização do algoritmo acima que “extrai” a reputação dos vértices em um grafo representando relações pessoas em redes sociais. Sabater e Sierra (2001) descrevem como experiência direta e feedback implícito e explícito podem ser combinados em um único mecanismo de reputação.

Basear a criação de reputação em informação implícita é uma solução promissora para os problemas de solicitar feedback confiável e em grande quantidade. A modelagem cuidadosa dos benefícios e limitações dessa abordagem é necessária para determinar em que condições ela pode ser um substituto viável, ou um complemento, para sistemas tradicionais de feedback.

4.4.2 Arquiteturas descentralizados de reputação

Descentralizar as fontes de feedback é uma abordagem promissora para atingir robustez em um mecanismo de reputação onde os mediadores são potencialmente desonestos e a privacidade é uma preocupação. Vários sistemas descentralizados foram propostos (Zacharia, Moukas *et al.*, 1999; Mui, Szolovits *et al.*, 2001; Sen e Sajja, 2002; Yu e Singh, 2002).

O surgimento de redes peer-to-peer provê uma motivação adicional ao desenvolvimento de mecanismos descentralizados de reputação. Em tais redes mecanismos de feedback constituem uma abordagem promissora para induzir a cooperação entre os nós participantes. Tentativas iniciais para desenvolver tais mecanismos foram reportadas por Aberer e Despotovic (2001) e Kamvar et al. (2003).

Mesmo envolventes e instigantes nenhum desses trabalhos provê uma análise rigorosa do comportamento induzido pelos mecanismos propostos, nem uma discussão sobre suas vantagens frente a outros mecanismos já estabelecidos. Mais colaboração se faz necessária nessa interação promissora entre cientistas da computação, que entendem as novas possibilidades oferecidas pelo avanço da tecnologia, e economistas, que melhor entendem o ferramental necessário para avaliar o potencial impacto de tais sistemas.

O objetivo do projeto de mecanismos de reputação online deve ser o de induzir um comportamento em uma comunidade com a precisão de quem constrói pontes. Isso, em conseqüência, requer uma modelagem precisa, não só dos

aspectos tecnológicos desses sistemas, mas também do comportamento de seus usuários dentro de seus respectivos grupos.

É bem conhecido que o comportamento humano não condiz com as previsões da economia tradicional, que prega que os usuários estão em constante busca da maximização de uma função de lucro pessoal bem definida (Rabin, 2003). Dois experimentos recentes provêm uma noção sobre o comportamento humano frente a mecanismos de reputação. Rabin compara bolsas de valores tradicionais com uma bolsa imaginária onde os mecanismos de feedback são gerados automaticamente. Ele concluiu que enquanto um mecanismo de feedback automático pode, sim, induzir uma melhora significativa na eficácia da troca de ações, ainda assim ele se sai muito pior que mecanismos reais, ou seja, não automatizados. Já Keser (2002) reporta os resultados de um jogo de confiança repetido entre estranhos com e sem a habilidade de fornecer feedback. Ela conclui que a presença de feedback não só aumenta significativamente os níveis de confiança e de confiabilidade como também a eficiência é maior quando ambas as partes de uma transação possuem o conhecimento da média global de confiança no sistema, e não apenas da confiabilidade dos seus parceiros.

5 Estudo de caso: Comunidade Stack Overflow

O Stack Overflow é um site de perguntas e respostas sobre programação. Ele cobre toda a área da programação, desde perguntas específicas sobre algum tópico a discussão de boas práticas para a construção de software.

Seu principal uso é perguntar e responder dúvidas e, através de participação ativa dos membros da comunidade, poder votar positivamente ou negativamente em uma pergunta ou resposta. A teoria por trás é que se uma resposta for suficientemente boa, ela terá mais votos que uma resposta ruim. Durante a exibição de uma pergunta, as respostas são ordenadas por votos. Sendo assim, a primeira resposta foi a mais votada, e conseqüentemente a mais provável de ser correta.

Esse conceito de votos pela comunidade não é particularmente novo, mas foi particularmente bem adotado no Stack Overflow, onde foi alinhado a um modelo de reputação interessante.

5.1 Distribuição da reputação na comunidade

Um aspecto interessante do site Stack Overflow é a importância que ele dá para a reputação, uma vez que utiliza ela como fator de autorização durante a interação entre o usuário e o site.

Todo o conteúdo do site, bem como informações sobre a reputação dos seus membros, está disponível de forma aberta para *download* em <<http://blog.stackoverflow.com/2009/06/stack-overflow-creative-commons-data-dump/>>.

A partir desse conteúdo, foram extraídas informações sobre a distribuição da reputação dos usuários dessa comunidade.

Na figura 7 temos, no eixo vertical, em escala logarítmica, o número de usuários, e no eixo horizontal a quantidade de reputação que um usuário tem.

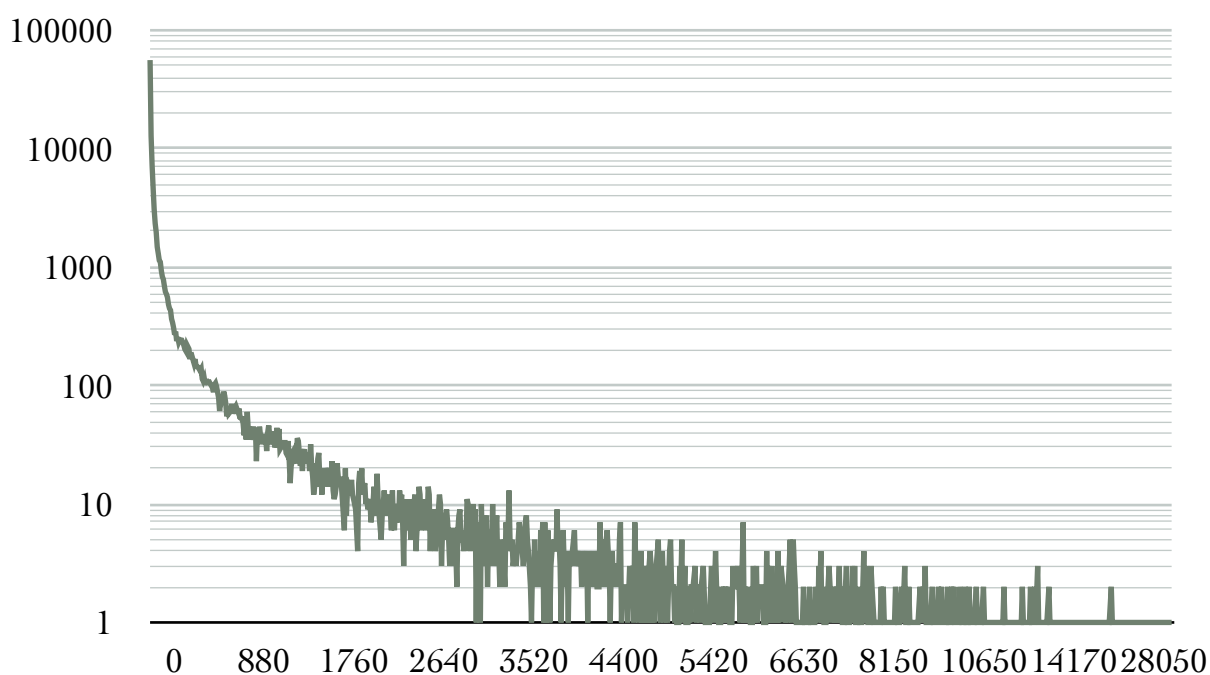


Figura 7 - Distribuição da reputação no site Stack Overflow

Tem-se então um comportamento já esperado: que a maioria dos usuários, nesse acaso mais da metade, possui menos de 100 pontos de reputação. Isso significa um usuário casual do site, que possivelmente faz uma pergunta específica e se avalia as respostas, mas que não sai ativamente respondendo perguntas de terceiros.

Já na outra ponta temos o “efeito cauda longa” onde um número cada vez menor de usuários possui uma grande reputação. Como ponto fora do gráfico, não

representado por motivos de escala, temos um usuário que realmente se destaca, possuindo mais de cem mil pontos de reputação. Esse usuário em particular é um autor famoso de livros de programação, e transferiu todo o conteúdo e interação do seu fórum para o site, aumentando o tráfego e a visibilidade do seu trabalho.

O site Stack Overflow é especialmente propício para o estudo proposto pois nele cada ação que um usuário pode executar, exige um mínimo de reputação, de acordo com a Tabela 1:

Ação	Reputação exigida
Votar positivamente	15
Marcar uma questão como ofensiva	15
Deixar um comentário	50
Votar negativamente	100
Editar perguntas comunitárias	100
Votar para remover sua própria pergunta	100
Criar uma nova seção do site	250
Renomear uma seção existente	500
Editar perguntas de outros usuários	2000
Votar para remover perguntas de outros usuários	3000
Acesso a ferramentas de moderação	10000

Tabela 1 - Reputação exigida para funções do site

Esse é um claro uso de reputação como fator autorizador. Ou seja, uma vez que certificamos que o usuário é idôneo, podemos permitir um maior acesso à comunidade.

Reputação pode ser adquirida através de votos de outros usuários. Por exemplo, cada voto positivo em uma resposta gera 10 pontos de reputação para o autor da resposta. Cada voto negativo, custa 10 pontos para o autor. Sendo assim, quanto mais perguntas o autor responder, e quanto melhor for a resposta, mais

reputação ele terá. Caso atinja dez mil pontos, ele se torna um moderador, com acesso ilimitado ao site.

Interessante também é o estudo da distribuição da reputação por ação que o usuário pode executar dentro do site, de acordo com a Figura 8:

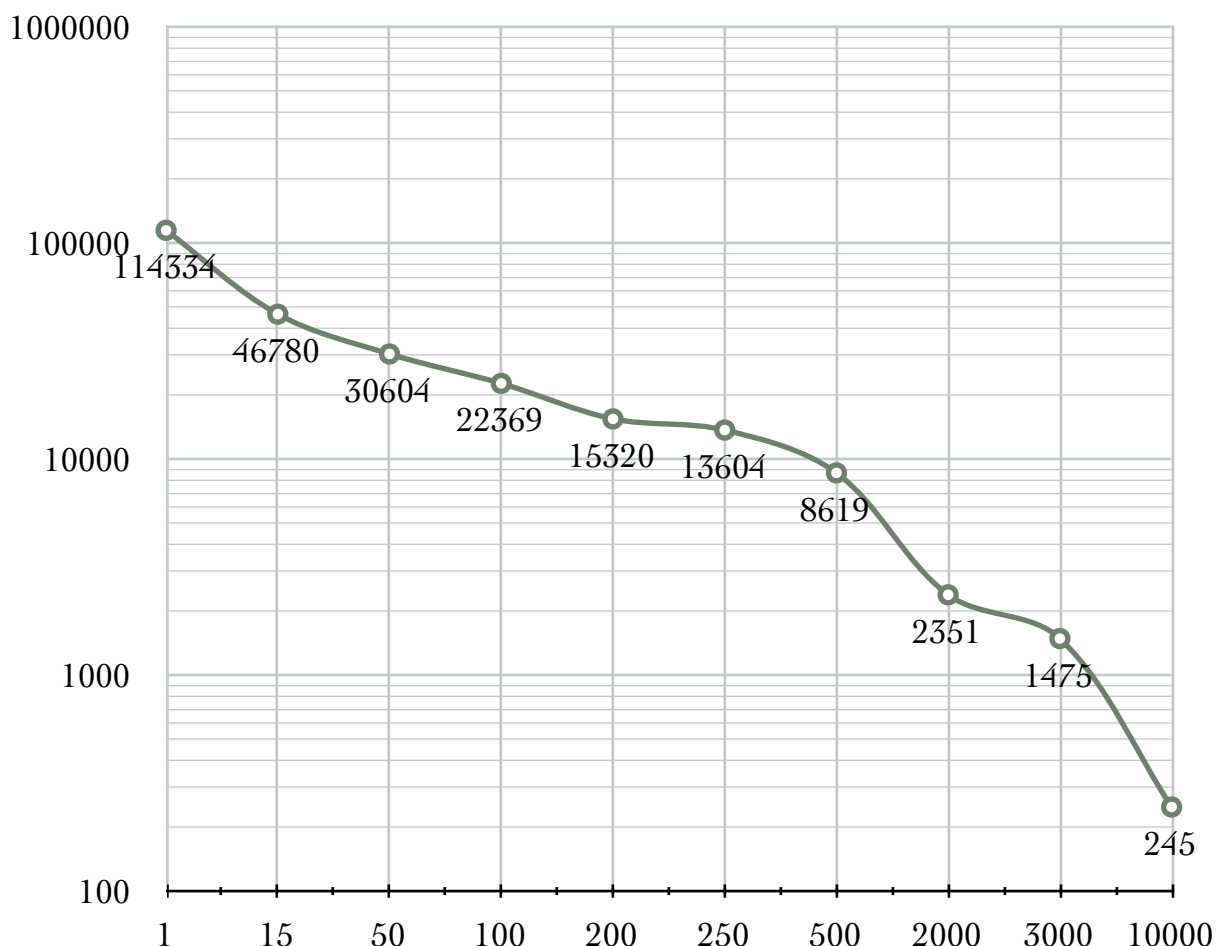


Figura 8 - Distribuição da reputação por ação autorizada

Aqui temos um gráfico cumulativo onde no eixo vertical, em escala logarítmica, é representado o número de usuários que possui reputação mínima para aquela uma ação, e no eixo horizontal o valor incremental da reputação, segmentado de acordo com a Tabela 1.

Como é observado a comunidade possuía em setembro de 2009 cerca de cento e quatorze mil usuários, dos quais apenas trinta mil são capazes de deixar comentários e apenas 245 possuem poder de moderação sob outros usuários.

Esse modelo é condizente com o esperado, onde alguns poucos usuários são altamente engajados, enquanto a maioria é caracterizada pelo uso casual.

5.2 Insígnias de reputação

Outra característica interessante do site Stack Overflow é a uso de insígnias, ou emblemas, como maneira de incentivar e agradecer um bom comportamento de um membro da comunidade.

Um bom sistema de reputação deve ter sido modelado de maneira a encorajar comportamentos desejados e tornar oneroso comportamentos vistos como não necessários ou dolosos para a comunidade. Para que os comportamentos desejados sejam ainda mais visíveis, apenas uma reputação numérica não basta.

Grupos sociais, como escoteiros, bombeiros e policiais, utilizam um sistema de medalhas desde sua formação. Quando um membro de um desses grupos realiza um ato que é considerado como exemplar, ganha uma medalha, que nada mais é do que um item que representa uma ação.

O objeto medalha em si não tem valor real, mas o seu significado é altamente valioso. Isso leva a crer que o significado de uma medalha de honra é meramente simbólico, e o valor de uma medalha está no reconhecimento que ela gera junto a seus pares (Fourquet, Larson *et al.*, 2006).

No site os emblemas podem ser divididos em 3 grandes categorias:

* Bronze: Insígnias de bronze são dadas ao usuários pelo uso normal do site. Elas encorajam as pessoas a usar as funções básicas do site como fazer perguntar, responder perguntas de terceiros, votar em perguntas e respostas, marcar uma pergunta como sendo de um tipo específico, preencher integralmente o perfil pessoal, etc. Insígnias de bronze são relativamente fáceis de conseguir e fornecem um *feedback* positivo imediato para um novo usuário;

* Prata: Insígnias de prata são para usuários já com experiência e premiam o uso contínuo do site. Elas encorajam o usuário a uma constante participação e foco em melhorar comunidade como um todo. Não são tão comuns quanto bronze, mas são alcançáveis, desde que o usuário se demonstre ativo; e

* Ouro: Insígnias de ouro são para os membros mais ativos da comunidade. Elas são concedidas apenas em casos especiais. Demonstram que um membro não é só participativo, mas também habilidoso e possui amplo conhecimento sobre algum tópico. São consideradas o pináculo da participação no site.

O ato de conceder uma medalha no Stack Overflow nunca é realizado de maneira arbitrária por um moderador. Elas são sempre concedidas ao se atingir um

objetivo numérico mensurável, disponível através de uma consulta à base de dados do site. Isso elimina a preocupação que um moderador privilegie um usuário específico através de medalhas, ou ainda que um usuário faça favores ao moderador para conseguir mais medalhas.

A maioria das insígnias disponíveis podem ser concedidas a um mesmo usuário múltiplas vezes, caso o comportamento seja observado múltiplas vezes.

Cada medalha possui um tipo, um nome e uma especificação, falando como é possível que um usuário receba ela. Abaixo na Tabela 1 podemos ver os tipos mais comuns de medalhas cedidas aos usuários:

Tipo	Nome	Ação
Bronze	Professor	Respondeu uma pergunta pela primeira vez
Bronze	Estudante	Fez uma pergunta pela primeira vez
Bronze	Editor	Editou pela primeira vez.
Bronze	Incentivador	Primeiro voto positivo
Bronze	Crítico	Primeiro voto negativo
Bronze	Bom cidadão	Marcou uma questão como ofensiva pela primeira vez
Prata	Bibliotecário	Reorganizou 100 perguntas
Prata	Anuário	Membro ativo por um ano
Prata	Generalista	Ativo em muitas áreas diferentes
Prata	Especialista	Altamente ativo em uma área específica
Prata	Guru	Teve a sua resposta escolhida como a melhor
Bronze	Boa pergunta	Fez uma pergunta que recebeu mais de 10 votos
Prata	Ótima pergunta	Fez uma pergunta que recebeu mais de 25 votos
Ouro	Excelente Pergunta	Fez uma pergunta que recebeu mais de 100 votos
Bronze	Pergunta interessante	Fez uma pergunta vista mais de 1.000 vezes
Prata	Pergunta fascinante	Fez uma pergunta vista mais de 2.500 vezes

Tipo	Nome	Ação
Ouro	Pergunta incrível	Fez uma pergunta vista mais de 10.000 vezes

Tabela 2 - Exemplo de insígnias no site Stack Overflow

Analizando a base de dados do site, é possível ver a distribuição das insígnias na comunidade:

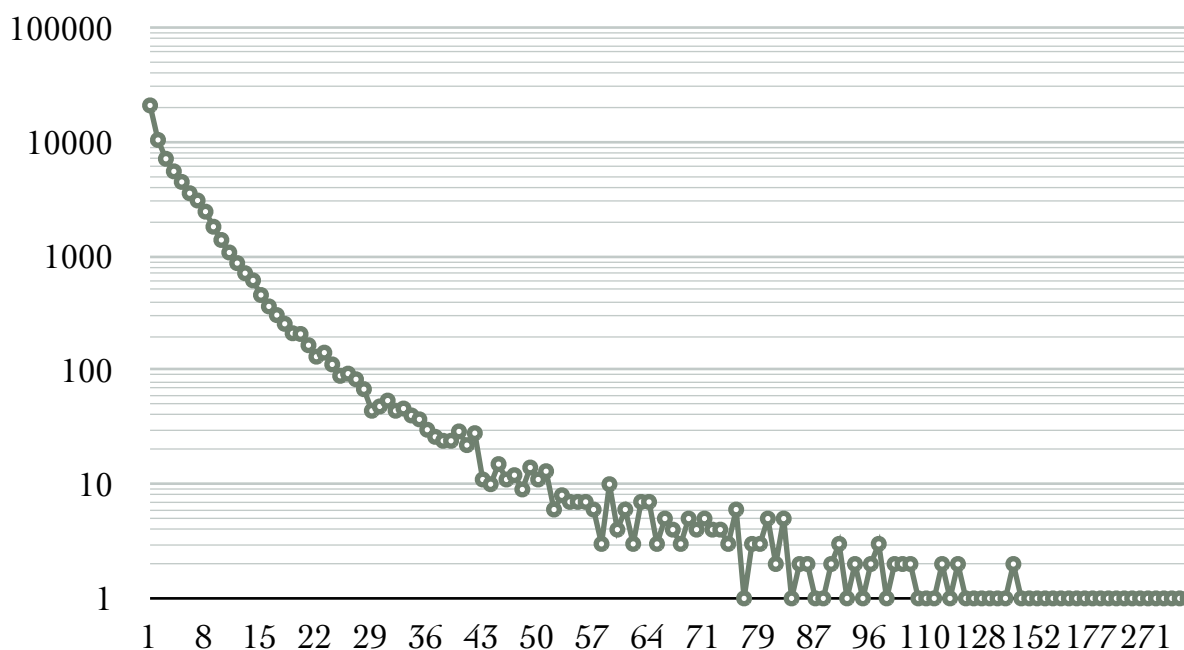


Figura 9 - Distribuição de insígnias no site Stack Overflow

Na figura 9 temos, no eixo vertical, o número de usuários em escala logarítmica, e no eixo horizontal o número de insígnias. Sendo assim, podemos observar a distribuição das insígnias na comunidade.

Como já é esperado, um grande número de usuários, 60 mil, possui até 10 insígnias. Esses são os usuários casuais do site, geralmente usam o site para perguntar alguma coisa ou ver a resposta de uma pergunta de terceiros, mas não participa ativamente, votando nas perguntas e respostas ou respondendo a perguntas de terceiro.

Temos em um outro extremo alguns usuários com mais de 100 insígnias. Não é coincidência que esses usuários tendem a ter mais de 10.000 pontos de reputação e se tornam moderadores. Eles são incrivelmente ativos na comunidade.

Dada uma alta correlação entre bons usuários, uma boa reputação e um bom número de insígnias, podemos adotar a modelagem de identidade do site Stack Overflow como base para a modelagem da reputação distribuída via OpenID.

6 Proposta de extensão: OpenID Reputation Exchange

OpenID Reputation Exchange é uma proposta de extensão de serviço para o protocolo OpenID com o intuito de possibilitar a troca de informação de reputação entre as Partes Confiantes.

Mensagens para recuperação do valor de reputação armazenado em uma Parte Confiante, recuperação da lista de Partes Confiantes disponíveis armazenada no provedor OpenID e registro de uma nova Parte Confiante perante o Provedor OpenID são especificadas.

6.1 Terminologia

As palavras-chaves "DEVE", "NÃO DEVE", "OBRIGATÓRIO", "DEVERÁ", "NÃO DEVERÁ", "RECOMENDADO", "PODE", e "OPCIONAL" no presente documento devem ser interpretadas como descrito na RFC2119.

6.1.1 Definições e Convenções

Usuário: Também designado “Usuário Final” ou “Sujeito”. Uma pessoa com uma identidade digital que participa em trocas de informações de identidade baseada em OpenID usando um cliente de software, normalmente um navegador web.

Identificador: Um identificador é qualquer URI "http" ou "https", (comumente referido como um "URL" no presente documento), ou um XRI [XRI_Syntax_2.0]. Deve ter sido normalizados de acordo com as regras da Seção de Normalização da especificação do OpenID 2.0.

Identificador Não Descoberto: Idêntico a um identificador, mas deve ser resolvido por meio do mecanismo descrito na Seção do Descobrimto do protocolo OpenID 2.0. O resultado da descoberta deve ser um identificador simples.

Provedor OpenID: Também chamado de "OP" ou "Servidor". Um servidor de autenticação OpenID no qual uma Parte Confiante confia para confirmar uma asserção que o usuário controla um identificador.

Parte Confiante: Também chamado de "RP", "Consumidor de identidade" ou "comunidade". Um aplicativo da Web que quer prova do controles de usuário final sob um identificador, e demanda os dados de identidade associados com o usuário final. Ele também avalia o comportamento do usuário final e classifica-o em conformidade.

Reputação: Um valor composto que indica quão valioso um usuário é paraa uma comunidade específica. Ele é bivalorado e contém uma parte numérica, que faz referência a uma classificação e um conjunto de emblemas de reputação, dados ao usuário quando o mesmo efetua um comportamento desejado.

Emblema de Reputação: Também conhecido apenas como "emblema". Atributo dado a um usuário que mapeia para um comportamento desejado dentro de uma comunidade. Atribuído quando uma ação positiva é realizada.

Todas as mensagens OpenID Reputation Exchange deve conter a seguinte declaração de espaço de extensão, conforme especificado na seção de extensões do protocolo OpenID 2.0:

```
openid.ns.<nome> = http://openid.net/srv/repx/1.0
```

O nome real da extensão deve ser atribuída a cada mensagem pela parte que compõe a mensagem, a fim de evitar conflitos entre as os nomes designados a múltiplas extensões, ou versões da mesma extensão. Para os fins deste documento, o nome da extensão para o serviço de troca de reputação será "repx".

6.2 Visão geral

O serviço de extensão para troca de informação sobre reputação é identificado pela URI "<http://openid.net/srv/repx/1.0>". Esta URI deve ser especificada na declaração do nome local atribuído à extensão.

Reputação é um atributo disperso associado a uma entidade identificada por um URI exclusivo e único. É composto por duas partes: um número e um conjunto de emblemas.

A parte numérica pode estar restrita a domínio de valores mínimos e máximos. Caso o domínio não seja explicitamente identificado DEVE ser assumido o domínio (0, Infinito). Quanto maior o valor numérico mais uma comunidade aprecia e

valoriza a participação do usuário. Emblemas são símbolos de gratidão concedidos por uma comunidade para um usuário final a fim de premiar o bom comportamento. Um emblema pode ser concedido múltiplas vezes para o mesmo usuário.

Esta proposta de extensão define três tipos de mensagens para a agregação e descoberta de reputação: `Fetch` (Seção 5), `List` (Seção 6) e `Add` (Seção 7).

`Fetch` recupera informações sobre a reputação armazenada em outra Parte Confiante sobre um determinado URI. `List` recupera uma lista do provedor de OpenID contendo Partes Confiantes válidas e que contenham alguma informação de reputação armazenada para aquele URI e `Add` salva ou atualiza uma nova Parte Confiante válida no Provedor de OpenID para que seja devolvido em uma mensagem `List` futura. Todas as mensagens são provenientes da Parte Confiante e são passadas para o provedor de OpenID, através do agente do usuário conforme a especificação do protocolo de autenticação OpenID.

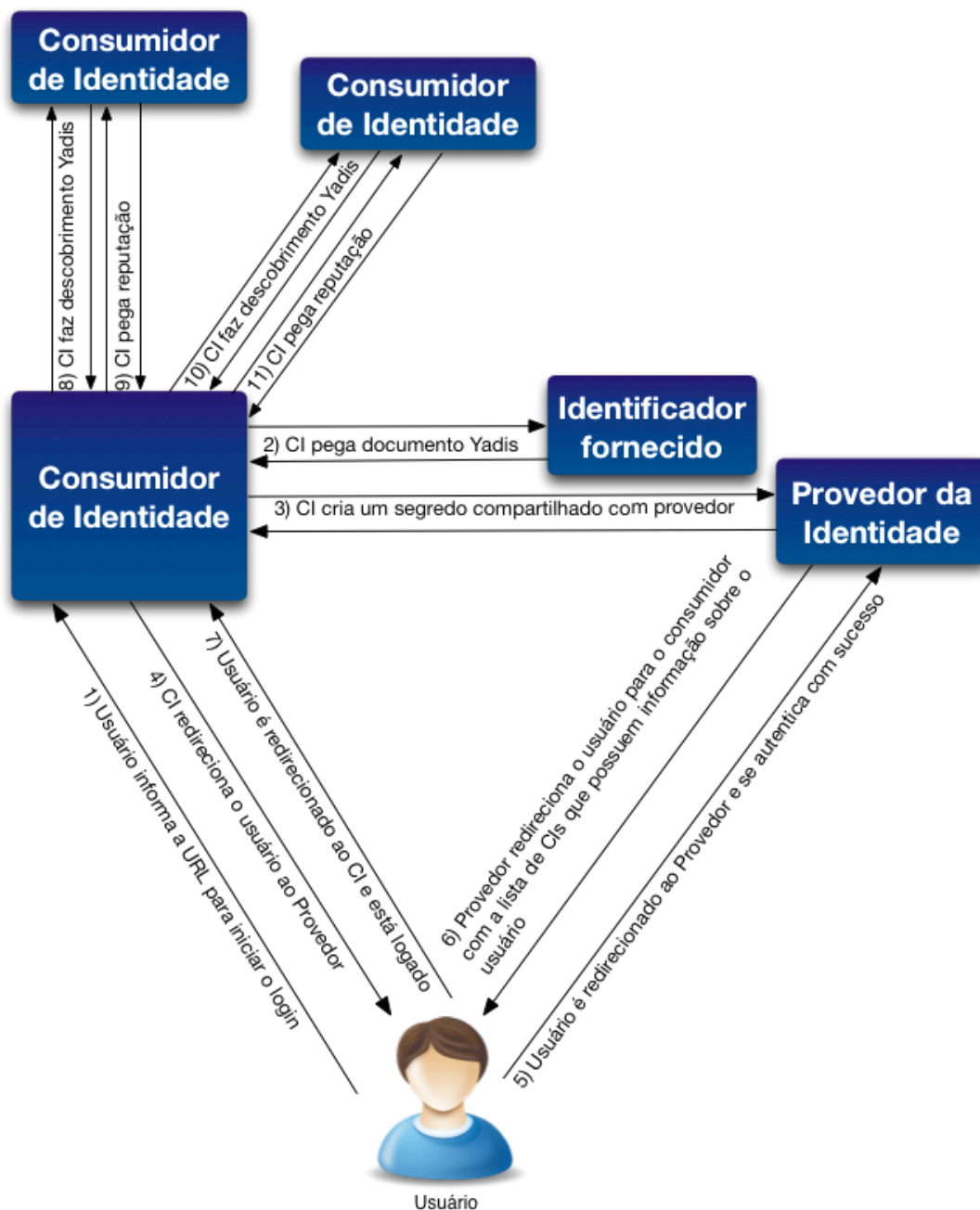


Figura 10 - Visão geral da interação com o protocolo OpenID 2.0

Todas as mensagens DEVEM ser realizadas com o emprego do mecanismo de Asserção Positiva do protocolo OpenID 2.0. Os parâmetros de solicitação detalhada aqui deve ser enviada com o emprego do mecanismo de extensão do protocolo OpenID 2.0.

6.3 Modelo de Informação

O proposta de extensão OpenID Reputation Exchange fornece um mecanismo para determinar o valor agregado de uma reputação, tanto na forma de um valor numérico como em um conjunto de emblemas:

- Um Valor de Reputação é associado com um identificador pessoal;
- Um Emblema de Reputação também está associado com um identificador pessoal;
- Um Emblema possui um identificador de tipo e uma contagem;
- Um identificador de tipo de um emblema é uma URI; e
- Uma contagem de tipo de emblema é o número de vezes que o emblema foi concedido ao usuário.

6.3.1. Identificador Pessoal

Representa um identificador pessoal não descoberto para um determinado usuário. Deve ser uma URI. O identificador pessoal corresponde ao identificador do usuário final na parte de autenticação das mensagens. Em outras palavras, o sujeito referenciado na parte de troca de informações sobre reputação é o mesmo usuário final referenciado na parte de autenticação da mensagem.

6.3.2. Valor de Reputação

A representação numérica da reputação deve ser um inteiro positivo. Seu limite superior deve ser o valor máximo representado por um número inteiro em 32 bits.

Devido à natureza dispersa da reputação, um usuário não possui um valor global desse atributo designada a ele. Para cada comunidade, o usuário pode ter um valor diferente de reputação. Um valor útil pode ser determinado pela combinação dos valores de outras comunidades de uma forma que seja pertinente para o agregador.

Uma comunidade PODE decidir aceitar informações de reputação provenientes apenas de outras comunidades nas quais confia.

6.3.3. Identificador de Tipo do Emblema de Reputação

Um identificador de tipo de emblema deve ser uma URI, que é usado para se referir a valores de propriedade.

Se um identificador de tipo de emblema pode ser resolvido então ele pode ser derreferenciado para obter uma descrição semântica do emblema. As Partes Confiantes podem utilizar os metadados obtidos através da descrição de um tipo de

emblema para, dinamicamente, inferir o significado de um emblema novo ou desconhecido e publicá-lo no perfil do usuário.

Isso proporciona a flexibilidade e extensibilidade. Flexibilidade no que ambos URIs e URLs pode ser usado para se referir a semântica de um emblema. Extensibilidade já que permite que qualquer comunidade, ou um consórcio de comunidades, possa definir seus próprios tipos de emblema, e especificar sua sintaxe e semântica.

Uma Parte Confiante PODE pode ignorar um ou mais emblemas caso considere que o emblema não é relevante ou aplicável para eles.

6.4 Descoberta

A descoberta da disponibilidade da extensão de troca de informação sobre reputação é realizada através do protocolo Yadis, conforme mecanismo descrito em OpenID 2.0. O espaço para troca de reputação "<http://openid.net/srv/repx/1.0>" DEVE ser listado como um elemento filho do elemento `<xrd:Type>` presente no elemento `<xrd:Service>` no documento de descoberta Yadis. Qualquer das Partes Confiantes de que deseja ser incluída na agregação de reputação deve permitir a descoberta na URI de troca de informação sobre reputação enviada ao Provedor OpenID como parte da mensagem Add.

6.5 Mensagem Fetch

A mensagem `Fetch` é usada para recuperar as informações sobre a reputação e o conjunto de emblemas de um usuário armazenados em uma Parte Confiante.

6.5.1 Formato da mensagem

Todos os campos pedido a seguir são OBRIGATÓRIOS, exceto "`openid.repx.offset.badge`" que deve ser usado se o conjunto de emblemas foi considerado demasiadamente grande para ser devolvido em uma única mensagem, e "`openid.repx.count.badge`" que pode ser ajustado para limitar o tamanho do conjunto de emblemas a ser retornado.

`openid.repx.mode`

OBRIGATÓRIO. Valor: "`fetch_request`".

openid.repx.offset.badge

OPCIONAL. Valor: um número inteiro positivo que informa o número de emblemas obtido anteriormente a este pedido.

Se estiver presente, o valor deve ser maior que zero. Se não presente deve ser considerada como "0".

openid.repx.count.badge

OPCIONAL. O número de tipos de emblema que a Parte Confiante que efetuou o pedido pretende receber da outra Parte Confiante como resposta.

Se estiver presente, o valor deve ser maior que zero, ou o valor especial "unlimited" que significa que o PR está solicitando todos os tipos de emblema que o outro RP tem associados naquele identificador pessoa. Se ausente, o valor deve ser considerado como "unlimited".

Partes Confiantes PODEM retornar um número menor ou igual de tipos de emblemas do valor especificado por este campo para o identificador associado, mas NÃO DEVE voltar mais do que o número de tipos de emblema solicitado para o identificador.

Este é um exemplo de uma mensagem Fetch. Neste caso, já foram obtidos anteriormente 10 emblemas, conforme inferível pelo no parâmetro "openid.repx.offset.badge" e está solicitando mais 10, conforme especificado no parâmetro "openid.repx.count.badge". A ordem dos emblemas tem de ser constante e, como tal, um RP PODE presumir que não muda entre os pedidos e o deslocamento será sempre um ponto de continuação válido do conjunto anterior.

```
openid.ns.repx = http://openid.net/srv/repx/1.0
fetch_request openid.repx.mode =
openid.repx.count.badge = 10
openid.repx.offset.badge = 10
```


6.5.2 Formato da resposta

6.5.2.1 Sucesso

A mensagem de resposta para uma mensagem `Fetch` informa a reputação localmente armazenada conforme solicitado. Cada emblema é fornecido com um nome canônico e atribuído como valor do prefixo “alias” do parâmetro `"openid.repx.badge.<alias>"`. A URI que especifica o tipo do emblema deve ser o valor atribuído a esse parâmetro. O comprimento mínimo para o prefixo “alias” suportado para um emblema DEVE ser de pelo menos 32 caracteres.

Com exceção de `"openid.repx.mode"` e `"openid.repx.reputation"`, todos os campos de pedido que se seguem são de caráter OPCIONAL, embora qualquer emblema presente em um parâmetro `"openid.repx.badge.<alias>*"` deve ter um também presente um parâmetro `"openid.repx.badge.<alias>"` associado.

A posição de um emblema distinto no conjunto deve ser constante entre requisições, a fim de afirmar a validade do parâmetro `"offset.badge parâmetro"`. O conjunto de emblemas pode ser ordenada da maneira que mais agrada a Parte Confiante, desde que siga o requerimento acima descrito.

openid.repx.mode

OBRIGATÓRIO. Valor: `"fetch_response_success"`.

openid.repx.reputation

OBRIGATÓRIO. O valor numérico para a reputação.

openid.repx.reputation.step

OPCIONAL. O valor numérico do incremento comumente aplicado a reputação.

Qualquer ação comum valiosa para uma comunidade provavelmente aumentará o valor da reputação de um usuário por este valor.

Por exemplo, dentro de uma comunidade Open Source com uma `step` de 10, arrumar um erro presente no gerenciador de erros do projeto pode dar ao usuário 10 pontos de reputação. Arrumar um erro particularmente difícil pode dar-lhe 35 pontos

de uma vez só. Já que nem todos os erros são particularmente difíceis podemos considerar o passo como 10.

Se estiver presente, o valor deve ser maior que zero e menor que "openid.repx.reputation.limit". Se ausente, o valor deve ser considerado "1".

openid.repx.reputation.limit

OPCIONAL. O valor numérico máximo para a reputação.

Se estiver presente, o valor deve ser maior que zero, ou o especial valor "unlimited", que significa que o valor máximo permitido é o maior valor representável por um inteiro de 32 bits. Se ausente, o valor deve ser considerado como "unlimited".

openid.repx.reputation.start

OPCIONAL. O valor numérico mínimo para a reputação.

Se estiver presente, o valor deve ser maior que zero. Se ausente, o valor deve ser considerado "0".

openid.repx.offset.badge

OPCIONAL. Valor: Um número inteiro positivo que informa a quantidade de emblemas obtido em requisições anteriores a essa.

Se estiver presente, o valor deve ser maior que zero. Se não estiver presente ela deve ser considerada como "0".

openid.repx.count.badge

OBRIGATÓRIO. O número de tipos de emblemas associados ao identificador que estão armazenados na Parte Confiante que responde ao pedido. O valor deve ser maior ou igual a zero.

openid.repx.badge.<alias>

OPCIONAL. URI usada para identificar o tipo de emblema. O valor de <alias> continuará a ser usado para identificar o tipo de emblema que está sendo trocado durante toda a mensagem.

O valor de <alias> não deve conter caracteres de nova linha e dois pontos, conforme especificou-se na sessão Formato de Mensagens de Dados do protocolo OpenID 2.0, mas também não deve conter vírgulas (",") e pontos (".").

openid.repx.badge.<alias>.count

OPCIONAL. Número de vezes que o emblema foi atribuído ao usuário. Se ausente, o emblema foi atribuído exatamente uma vez.

openid.repx.badge.<alias>.name

OPCIONAL. Nome alternativo para o emblema. Se ausente o nome DEVE ser inferido através da capitalização da primeira letra de <alias>. O nome pode ser específico de uma comunidade.

O valor do nome deve ser uma seqüência de caracteres no formato UTF-8 [RFC3629]. A fim de adequar-se formatos de dados definidos pelo protocolo OpenID 2.0, não deve conter novas linhas (UCS codepoint 10, "\n").

Abaixo segue a resposta ao pedido de exemplo anterior. Como pode ser visto 10 emblemas já foram transferidos. Os restantes 7 emblemas estão sendo transferidos nessa resposta:

```
openid.ns.repx=http://openid.net/srv/repx/1.0
openid.repx.mode=fetch_response_success
openid.repx.reputation=616
openid.repx.reputation.step=10
openid.repx.reputation.limit=10000
openid.repx.reputation.start=10
openid.repx.count.badge=17
openid.repx.offset.badge=10
openid.repx.badge.committer=http://example.com/schema/committer
openid.repx.badge.committer.name=Committer on Trunk
openid.repx.badge.commentator=http://example.com/schema/commentator
openid.repx.badge.commentator.count=3
openid.repx.badge.yearling=http://example.com/schema/yearling
openid.repx.badge.yearling.name=Active Member
openid.repx.badge.yearling.count=2
openid.repx.badge.organizer=http://example.com/schema/organizer
openid.repx.badge.scholar=http://example.com/schema/scholar
```

```
openid.repx.badge.student=http://example.com/schema/student  
openid.repx.badge.supporter=http://example.com/schema/supporter
```

6.5.2.2 Falha

A mensagem de resposta em caso de falha tem o seguinte formato:

openid.repx.mode

OBRIGATÓRIO. Valor: "fetch_response_failure".

openid.repx.error

OPCIONAL. Parâmetro que descreve a condição de erro que induziu a resposta ao fracasso. Deve ser destinada a ser apresentada ao usuário. A localidade da mensagem deve coincidir com a localidade da mensagem HTTP.

Exemplo de erro genérico. Nesta instância, quando o usuário não está mais presente na comunidade.

```
openid.ns.repx = http://openid.net/srv/repx/1.0  
openid.repx.mode = fetch_response_failure  
openid.repx.error = Identificador não presente no sistema
```

6.6 Mensagem List

A mensagem `List` é usada para informar uma Parte Confiante sobre outras Partes Confiantes que também contém informações sobre a reputação do identificador fornecido.

Esta mensagem é proveniente de uma Terceira Parte de um provedor de OpenID, que responde com a lista. A lista pode ser restrita a um subconjunto das Partes Confiantes o provedor OpenID possuem para esse identificador, permitindo ao utilizador escolher quem conhecerá sua reputação como um todo.

6.6.1 Lista Pedido Formato

openid.repx.mode

OBRIGATÓRIO. Valor: "list_request".

openid.repx.endpoint.count

OPCIONAL. Número de Partes Confiantes desejado para agregar na reputação local do usuário.

Se estiver presente, o valor deve ser maior que zero, ou o valor especial "unlimited" que significa que o RP está solicitando o número total de RP atualmente associadas ao identificador presente nesse Provedor OpenID. Se ausente, o valor deve ser considerado como "unlimited".

O Provedor de OpenID pode voltar inferior ou o número exato de RP especificada por este campo para o identificador associado, mas não deve voltar mais do que o número de RP solicitados para o identificador.

```
openid.ns.repx = http://openid.net/srv/repx/1.0
```

```
list_request openid.repx.mode =
```

```
openid.repx.count = 5
```

6.6.2 Lista Response Format

6.6.2.1 Sucesso

O sucesso da mensagem de List é indicado pelo parâmetro "mode".

openid.repx.mode

OBRIGATÓRIO. Valor: "list_response_success".

openid.repx.endpoint.count

OBRIGATÓRIO. O número de Partes Confiantes que foram retornadas para o identificador. O valor deve ser maior ou igual a zero.

openid.repx.endpoint.<number>

Um identificador passível de descoberta que será consultado via mensagem `Fetch` para obtenção de informação sobre reputação.

O valor de `<number>` identifica o índice da Parte Confiante, que varia de um para o valor especificado por `"openid.repx.endpoint.count"`. Não é necessário preservar a ordem das Partes Confiantes enviadas entre respostas distintas da mensagem.

```
openid.ns.repx = http://openid.net/srv/repx/1.0
openid.repx.mode = list_response_success
openid.repx.endpoint.count = 3
openid.repx.endpoint.1 http://example.com =
openid.repx.endpoint.2 http://otherexample.com/endpoint =
openid.repx.endpoint.3 = http://another.example.comx
```

6.6.2.2 Falha

A resposta da mensagem `List` em caso de falhar tem o seguinte formato:

openid.repx.mode

OBRIGATÓRIO. Valor: `"list_response_failure"`.

openid.repx.error

OPCIONAL. Parâmetro que descreve a condição de erro que induziu a resposta ao fracasso. Deve ser destinada a ser apresentada ao usuário. A localidade da mensagem deve coincidir com a localidade da mensagem HTTP.

```
openid.ns.repx = http://openid.net/srv/repx/1.0
openid.repx.mode = list_response_failure
openid.repx.error = Identificador não reconhecido
```

6.7 Mensagem Add

A mensagem Add é usada para armazenar uma Parte Confiante como uma nova fonte de reputação no Provedor OpenID, que fornece os meios necessários para um RP calcular a reputação agregada de um usuário. O valor armazenado no OP deve ser um identificador passível de descoberta e capaz de tratar consultas de reputação através da mensagem Fetch.

6.7.1 Formato da mensagem Add

Todos os campos seguinte pedido são OBRIGATÓRIOS.

openid.repx.mode

Valor: "add_request".

openid.repx.endpoint

O valor deste parâmetro deve ser um identificador passível de descoberta, conforme anteriormente descrito.

Exemplo:

```
openid.ns.repx = http://openid.net/srv/repx/1.0  
add_request openid.repx.mode =  
http://example.com/op/endpoint openid.repx.endpoint =
```

6.7.2 Formato de resposta

6.7.2.1 Sucesso

O êxito da operação de adição é indicado pelo parâmetro "mode".

openid.repx.mode

OBRIGATÓRIO. Valor: "add_response_success".

```
openid.ns.repx = http://openid.net/srv/repx/1.0  
openid.repx.mode = add_response_success
```

6.7.2.2 Falha

Uma resposta a mensagem Add que indica falha tem o seguinte formato:

openid.repx.mode

OBRIGATÓRIO. Valor: "add_response_failure".

openid.repx.error

OPCIONAL. Parâmetro que descreve a condição de erro que induziu a resposta ao fracasso. Deve ser destinada a ser apresentada ao usuário. A localidade da mensagem deve coincidir com a localidade da mensagem HTTP.

```
openid.ns.repx = http://openid.net/srv/repx/1.0  
openid.repx.mode = add_response_failure  
openid.repx.error = Não permitida a participação
```

6.8 Considerações de Segurança

OpenID Reputation Exchange é uma extensão do OpenID e, portanto, usa OpenID pedido de autenticação e mensagens de resposta para troca de informações com o provedor de OpenID. Reputação é um atributo disperso e é atribuído e hospedado por Partes Confiantes. Ela caracteriza a informação pública, e como tal não está sujeita às questões de segurança, mas tem preocupações com a privacidade. A questão da segurança da informação trocada no protocolo pode ser vista na seção "Considerações sobre Segurança" da norma OpenID Authentication 2.0.

8. Conclusões e trabalhos futuros

O uso de reputação como ferramenta de autorização para comunidades geograficamente dispersas já comum há diversos anos. Mesmo assim a falta de integração entre a informação de reputação e protocolos Single Sign On foi surpreendente.

As possibilidades desse tipo de sistema são instigantes. Comunidades que confiam umas nas outras podem utilizar esse ferramental como uma maneira padronizada de troca de mensagens sobre o comportamento de um usuário que participa ativamente em ambas. É ainda mais relevante a possibilidade de um usuário poder iniciar seu engajamento com uma comunidade sem que seja necessário seguir toda a escalada de reputação a partir do começo, já que ele demonstrou previamente o seu valor para outra comunidade.

Isso é uma grande vantagem, especialmente para comunidades de código livre, onde todos se beneficiam caso um usuário participe em múltiplas comunidades. Considerando essa vantagem, e a falta de uma proposta já existente, semelhante à apresentada nesse trabalho, põe em dúvida sua viabilidade prática.

Talvez o maior empecilho para a implantação de tais sistemas seria a possível redução de privacidade causada pelo uso de uma URI identificadora não só para atributos determinados pelo usuário, mas também para atributos adicionados por uma terceira parte.

Aqui entra um fator decisivo na criação do protocolo OpenID: que o usuário deveria controlar todas e quaisquer informações relacionadas a uma URI. Isso é contraditório com o processo identitário, onde o significativo é o que uma comunidade, como entidade coletiva, pensa a respeito de um indivíduo.

Mesmo assim, esse trabalho se demonstra promissor, já que apresenta uma maneira do usuário controlar quem participa da agregação da sua reputação, mitigando assim a preocupação com a privacidade.

O protocolo é simples e de fácil implementação, devido ao uso do protocolo base para as tarefas mais árduas.

Como trabalhos futuros pode-se ter o envio da especificação do protocolo ao OpenID.net, grupo que controla a especificação de tudo ligado ao OpenID, bem como suas extensões.

Referências bibliográficas

ABERER, K. e DESPOTOVIC, Z. Managing trust in a peer-2-peer information system. Proceedings of the tenth international conference on Information and knowledge management. Atlanta, Georgia, USA: ACM 2001.

AVERY, C., RESNICK, P., *et al.* The market for evaluations. American Economic Review, v.89, n.3, p.564-584. 1999.

BAJARI, P. e HORTACSU, A. Winner's curse, reserve prices and endogenous entry: Empirical insights from ebay auctions. Econometric Society World Congress: Econometric Society 2000.

BERNERS-LEE, T., MASINTER, L., *et al.* Uniform resource locators (url). RFC. 1738 1994.

BHARGAV-SPANTZEL, A., CAMENISCH, J., *et al.* User centricity: A taxonomy and open issues. Proceedings of the second ACM workshop on Digital identity management. Alexandria, Virginia, USA: ACM 2006.

BRIN, S. e PAGE, L. The anatomy of a large-scale hypertextual web search engine. Comput. Netw. ISDN Syst., v.30, n.1-7, p.107-117. 1998.

CAMERON, K. The laws of identity 2005.

CAMP, J. L. Digital identity. Technology and Society Magazine, IEEE, v.23, n.3, 2004-10-04, p.34-41. 2004.

CANTOR, S. Assertions and protocols for the oasis security assertion markup language (saml) v2.0. OASIS Standard 2005.

DELLAROCAS, C. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. Proceedings of the 2nd ACM conference on Electronic commerce. Minneapolis, Minnesota, United States: ACM 2000.

_____. Analyzing the economic efficiency of ebay-like online reputation reporting mechanisms. Proceedings of the 3rd ACM conference on Electronic Commerce. Tampa, Florida, USA: ACM 2001a.

_____. Building trust on-line: The design of reliable reputation reporting : Mechanisms for online trading communities. MIT Sloan, v.4180, n.01. 2001b.

DEWAN, S. e HSU, V. Adverse selection in electronic markets: Evidence from online stamp auctions. Journal of Industrial Economics, v.52, n.4, p.19. 2004.

DIAMOND, D. W. Reputation acquisition in debt markets. Journal of Political Economy, v.97, n.4, p.828-62. 1989.

DRANOVE, D., KESSLER, D. P., *et al.* Is more information better? The effects of 'report cards' on health care providers. Journal of Political Economy, v.111. 2003.

DUBAR, C. A socialização: Construção das identidades sociais e profissionais. São Paulo: Martins Fontes. 2005. 343 p.

FOURQUET, E., LARSON, K., *et al.* A reputation mechanism for layered communities. SIGecom Exch., v.6, n.1, p.11-22. 2006.

FRIEDMAN, E. J. e RESNICK, P. The social cost of cheap pseudonyms. Journal of Economics & Management Strategy, v.10, n.2, p.173-199. 2001.

HARDT, D. Openid attribute exchange 1.0. OpenID.net 2006.

HOLMSTROM, B. Managerial incentive problems: A dynamic perspective. National Bureau of Economic Research, IncJan. 1999

HOUSER, D. e WOODERS, J. C. Reputation in auctions: Theory, and evidence from ebay. Journal of Economics & Management Strategy, Vol. 15, pp. 353-369, Summer 2006.

KAMVAR, S. D., SCHLOSSER, M. T., *et al.* The eigentrust algorithm for reputation management in p2p networks. Proceedings of the 12th international conference on World Wide Web. Budapest, Hungary: ACM 2003.

KESER, C. Trust and reputation building in e-commerce. CIRANOJul. 2002

KREPS, D. e WILSON, R. Reputation and imperfect information. David K. LevineMay. 1999

KREPS, D. M., MILGROM, P., *et al.* Rational cooperation in the finitely repeated prisoners' dilemma. Journal of Economic Theory, v.27, n.2, p.245-252. 1982.

LUCKING-REILEY, D., BRYAN, D., *et al.* Pennies from ebay: The determinants of price in online auctions. Department of Economics, Vanderbilt UniversityNov. 1999

MAYZLIN, D. Promotional chat on the internet. Marketing Science, v.25, n.2, p. 155-163. 2006.

MILGROM, P., NORTH, D., *et al.* The role of institutions in the revival of trade: The law merchant, private judges, and the champagne fairs. Economics & Politics, v.2, n. 1, p.1-23. 1990.

MILLER, J. Yadis 1.0 2006.

MITJAVILA, M. R. Identidad social y comunidad. Notas acerca de las conexiones entre ambos conceptos. Cuadernos Del Claeh, v.3, p.67-77. 1994.

MUI, L., SZOLOVITS, P., *et al.* Collaborative sanctioning: Applications in restaurant recommendations based on reputation. Proceedings of the fifth international conference on Autonomous agents. Montreal, Quebec, Canada: ACM 2001.

PUJOL, J. M., SANGESA, R., *et al.* Extracting reputation in multi agent systems by means of social network topology. Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1. Bologna, Italy: ACM 2002.

RABIN, M. A perspective on psychology and economics. Economic Literature, v.36, Mar, p.11-46. 2003.

RECORDON, D. e FITZPATRICK, B. Openid authentication 1.1 2006.

RECORDON, D. e REED, D. Openid 2.0: A platform for user-centric identity management. Proceedings of the second ACM workshop on Digital identity management. Alexandria, Virginia, USA: ACM 2006.

REED, D. e MCALPIN, D. Extensible resource identifier syntax 2.0: OASIS Committee Specification

OASIS XRI Technical Committee 2005.

RESNICK, P., KUWABARA, K., *et al.* Reputation systems. Commun. ACM, v.43, n. 12, p.45-48. 2000.

SABATER, J. e SIERRA, C. Regret: Reputation in gregarious societies. Proceedings of the fifth international conference on Autonomous agents. Montreal, Quebec, Canada: ACM 2001.

SEN, S. e SAJJA, N. Robustness of reputation-based trust: Boolean case. Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1. Bologna, Italy: ACM 2002.

SHAPIRO, C. Consumer information, product quality, and seller reputation. Bell Journal of Economics, v.13, n.1, p.20-35. 1982.

TADELIS, S. The market for reputations as an incentive mechanism. SSRN eLibrary. 2001.

WACHOB, G. Extensible resource identifier resolution 2.0. OASIS Technical Committee 2005.

WIKIPEDIA Openid Disponível em <<http://en.wikipedia.org/w/index.php?title=OpenID&oldid=299595983>>. Acesso em: 01/07/2009

WILSON, R. Reputations in games and markets. Cambridge: Cambridge University Press. 1995. 62 p. (Game-theoretic models of bargaining)

YU, B. e SINGH, M. P. An evidential model of distributed reputation management. Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1. Bologna, Italy: ACM 2002.

ZACHARIA, G., MOUKAS, A., *et al.* Collaborative reputation mechanisms in electronic marketplaces. Proceedings of the Thirty-second Annual Hawaii International Conference on System Sciences-Volume 8 - Volume 8: IEEE Computer Society 1999.